COVERT COMMUNICATION OVER MULTI-USER CHANNELS

A Dissertation
Presented to
The Academic Faculty

By

Keerthi Suria Kumar Arumugam

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Electrical and Computer Engineering

Georgia Institute of Technology

May 2019

COVERT COMMUNICATION OVER MULTI-USER CHANNELS

Approved by:

Dr. John Barry, Committee Chair
Professor, School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Matthieu Bloch, Advisor
Associate Professor, School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Mary Ann Weitnauer
Professor, School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Mark Davenport
Associate Professor, School of Electrical and Computer Engineering
Georgia Institute of Technology

Dr. Sebastian Pokutta
Associate Professor, School of Industrial and Systems Engineering
Georgia Institute of Technology

Date Approved: March 26, 2019

தழல் வீரத்தில் குஞ்சென்றும் மூப்பென்றும் உண்டோ?

– பாரதி

To my partners in crime –

Siva, Sabari, and Lakshmi,

for their pats and shoulders.

ACKNOWLEDGEMENTS

First and foremost, I should thank my parents for their love and support. I still remember the several mornings when my mother would sit in the next room to keep me company at 3 AM while I studied for my exams. Ever since, all accomplishments have been a joint work with my mother. And, my father, who allowed me to make my own mistakes, never once questioned my life decisions, and provided extraordinary support over the years. I wish to thank my sister, my grandparents, my extended family, and all my friends, for their love and for all the happy memories.

I would like to thank my colleagues – Ishaque, Mehrdad, Alex, Rémi, Guillaume, Anne, and all others who have ever shared their workspace with me, for spoiling me with a peaceful environment and for answering every one of my silly questions. I am grateful to Victor and Sarwat for assuring me very early that I'll survive this journey; Bill and Warren, for keeping me honest and focused; David, for his extraordinary hospitality; and Eddie, without whom this pursuit would have been arduous. I also wish to sincerely thank Dr. Barry, Dr. Weitnauer, Dr. Davenport, and Dr. Pokutta for agreeing to be a part of my dissertation committee, and Dr. Ligong Wang for hosting me and sharing his expertise.

About five years ago, I met Dr. Bloch in his office to ask if he would advise my doctoral degree. Since that day, he has patiently let me explore unconfined, both inside and outside the lab. As one of our explorations together, he encouraged me to work on wireless radios and helped me realize the kind of work that I really enjoyed doing. Ultimately, I made career decisions based on this realization. For his unbelievable support, patience, and trust over all these years, I genuinely thank him. For years to come, I will continue to brag among friends that I had one of the coolest advisors ever.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

During World War I, a group of Belgian women famously helped the Allied forces defeat Germany in the first battle of Marne. With the German army marching aggressively towards the Western Front, the French and British forces required an estimate of the pace at which Germany was concentrating its troops and resources near the French border. Since every soldier, every can of food, and every piece of ammunition were transported by trains into Belgium, the Belgian resistance recruited women to knit this information onto sweaters. The women knitted, sitting at their windows, looking outside at the trains – a bumpy stitch for every wagon that carried troops and a dropped stitch for every wagon that carried resources. The sweaters were then handed over to a soldier from the resistance through merchants who carried these information-embedded sweaters among other regular sweaters to the market in full view of vigilant German soldiers. Thus, crucial information about the German arsenal was transmitted to France in plain sight using an unsuspected medium.

A few years later, during the height of the Cold War, CIA agents resorted to creative ways to transmit messages without attracting any attention since they were unaware if they were being watched. According to the recently declassified Cold War-era training manual for CIA field agents [1], the agents were trained to hide messages in shoelace patterns by modifying the way shoelaces were fed through the shoes' eyelets. Although alternate ways of tying shoelaces rarely attracted any unwanted attention, the patterns were easily perceived by other agents who were actively looking for such a signal. This way, the agents converted an often overlooked piece of apparel into a medium for signaling messages such as *I have information for you*, *I have brought another person with me*, and *Follow me*. Moreover, CIA agents were also

trained [1] to use the color of shirt buttons and placement of pen in shirt pockets to communicate without being detected.

Later, in 1966, the U.S. Office of Naval Intelligence confirmed for the first time that American prisoners of war were being mistreated in northern Vietnam after the broadcast of Admiral Jeremiah Denton's interview shot for propaganda purposes. The Northern Vietnamese Army had forbidden Denton from revealing the true conditions of the prison camp and had given him scripted answers about the treatment of prisoners in the camp. Although Denton stuck to the script for his answers in the video, he could be seen blinking uncomfortably every once in a while. When inquired about his strange actions, Denton feigned by citing trouble with the blinding spotlight. In fact, as the U.S. intelligence would later reveal, Admiral Jeremiah Denton had spelled out T-O-R-T-U-R-E by blinking his eyes in a Morse code pattern. Denton had used his television appearance and innocuous verbal answers as the medium to hide his one-word message to the world. Numerous other incidents in history [2] have called for a means to communicate without being detected.

In all the above cases, the adversary failed to identify the presence of a hidden message because he was not actively looking for it. To put it in simple words, the message remained hidden only because the adversary was not aware of the medium in which the message was embedded. However, according to *Kerchkoff's principle* or *Shannon's maxim* [3], the adversary should possess the same knowledge of the information-hiding scheme as the parties involved in the communication with the exception of a secret key, if any. In many scenarios, the very intention to transmit information is considered an act of breach and could result in the adversary shutting down the channel and punishing the users. Simmons introduced one such scenario as the prisoners' problem [4], in which two prisoners exchange messages in the hope that they can coordinate to devise an escape plan while a warden monitors the communication and only allows the transmission of innocuous messages. On detection of

the presence of any non-innocuous message, the warden will punish both prisoners and send them to separate high-security prisons for the rest of their lives irrespective of the content of their messages.

In this work, we address the general problem of computing the maximum rate at which information can be transmitted over certain multi-user channels while simultaneously escaping detection from an adversary. We also address the advantage gained by ensuring that the adversary is not synchronized with the covert transmitter. This work is organized as follows. In Chapter 2, we discuss previous works related to various information-hiding schemes and Low Probability of Detection (LPD) communication, and also review a mathematical framework to analyze LPD communication. Chapters 3, 4, and 5, detail our results on covert communication over multiple-access, broadcast, and relay channels, respectively. Chapter 6 presents our results on asynchronous covert communication.

CHAPTER 2

LITERATURE SURVEY

2.1 Information-hiding schemes

As mentioned in the previous chapter, in certain scenarios, users are required to keep their transmission status a secret. In such situations, obscuring a message by encryption does not suffice since the very presence of an encrypted message gives away the presence of a message. For instance, the existence of encrypted communication between an individual and an adversarial foreign government reveals the possibility of espionage. Consequently, a necessity to use techniques other than encryption arises to hide the status of transmission. Techniques commonly associated with undetectable communication include steganography and spread spectrum communication.

2.1.1 Steganography

Steganography, derived from the Greek word $\sigma\tau\epsilon\gamma\alpha\nu\omega$ meaning *concealed writing*, is an information-hiding scheme that conceals a message in an innocent-looking *covertext*. The transmitter embeds the message[1] in the covertext to produce a *stegotext*. The adversary[2] with the knowledge of the properties of the covertext attempts to detect the presence of a message. A stegotext that closely resembles the covertext hinders the adversary from detecting the presence of the message. As an example, Figure 2.1(a) illustrates an image of Claude Shannon and serves as our cover image. Figure 2.1(b) illustrates[3] the cover image embedded with a payload of 1093 words. Although the two images look identical on visual inspection, we illustrate the en-

[1] *plaintext* or an encrypted plaintext (*ciphertext*)

[2] An adversary may either be active or passive. While both attempt to detect the presence of a message, the former also attempts to remove or modify the embedded message. Henceforth, we only discuss passive adversaries throughout this document.

[3] Message embedded using *steghide 0.5.1*.

(a) Cover image (b) Message-embedded image (c) Enhanced difference

Figure 2.1: Image steganography

hanced difference between the two images in Figure 2.1(c). This particular image steganographic technique works by identifying pairs of pixels whose exchange would embed the message while remaining undetectable to basic statistical tests. However, several other simple embedding schemes are dreadful in hiding messages even from adversaries using basic statistical tests. For instance, sequential steganography [5], which involves embedding the message in consecutive samples, can be detected by a simple cumulative-sum test [6] because of the abrupt change in local statistics.

To design well-performing steganographic techniques, it is necessary to compute the maximum amount of information that can be hidden in a given covertext. While Maurer [7] first drew the connection between steganography and *hypothesis testing*, Cachin introduced an information-theoretic model for steganography [8] by proposing an adversary who estimates the presence of an embedded message using a metric that only depends on the statistics of the stegotext and the covertext. Subsequently, Ker studied batch steganography [9], in which the payload is spread across n different cover objects each with the same capacity, and he observed that the throughput scales on the order of $\sqrt{n}$. He also showed [10] that a linear increase in the message length with the number of cover objects leads to detection at the adversary. Specifically, the *square-root law* of steganography [11] states that at most $\mathcal{O}(\sqrt{n})$ bits can be hidden in a covertext of size n. While Ker [12] showed that steganography can be

achieved using a secret key on the order of the size of the payload, he also rendered the secret key unnecessary in certain cases by widely spreading the possible payload locations in a large cover [13]. Unlike previous works [9, 10] that used independent and identically distributed (i.i.d.) cover objects to embed information, Filler *et al.* [14] analyzed steganography using Markovian covers since i.i.d. covers do not capture the inter-dependence that is a characteristic of commonly-used covers such as images and video frames. A few other works [15, 16] have showed that embedding messages in a transform space rather than in the actual covertext is also subject to the square-root law.

2.1.2 Spread spectrum techniques

To avoid detection, defense systems around the world use *spread spectrum* techniques [17]. Specifically, Direct Sequence Spread Spectrum (DSSS) communication techniques spread a signal of bandwidth W_M over a much wider bandwidth $W_S \gg W_M$ using a high frequency pseudo-random chip sequence, thus ultimately reducing the Power Spectral Density (PSD) of the signal to be close to the PSD of the noise [18]. Consequently, DSSS signals are immune from adversaries employing energy detection [19] or narrowband signal detection [20]. However, contrary to popular belief, DSSS signals can be detected by adversaries using autocorrelation- and cyclic feature-based detectors [21, 22, 23]. Although Chuang *et al.* [24] improved upon conventional spread spectrum techniques by using noise-modulation techniques to prevent detection by conventional receivers, Bash *et al.* [25] showed that spread spectrum communication is also subject to the *square-root law* if the communication is to be fundamentally undetectable from the adversary.

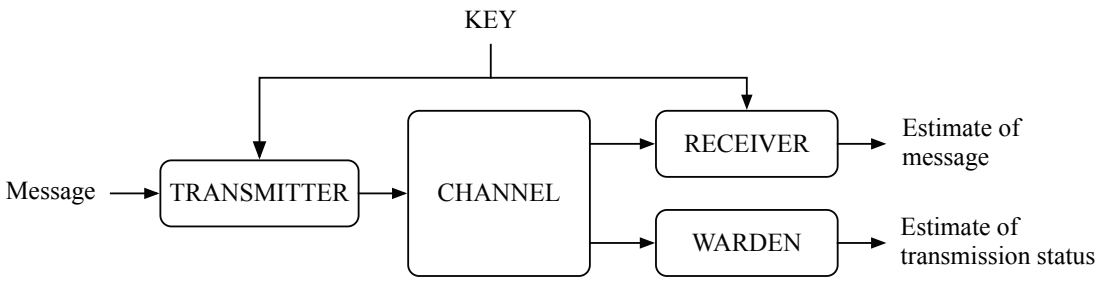

Figure 2.2: Communication in the presence of a warden

2.2 Covert communication

The problem of covert communication can be formalized using the communication model illustrated in Figure 2.2, in which the transmitter communicates a message to the legitimate receiver with the help of a secret key[4] while preventing the warden from correctly estimating the status of transmission. Prior to discussing the model mathematically in Section 2.2.2, we first introduce the notation used throughout the document.

2.2.1 Notation

We denote random variables and their realizations in upper and lower case, respectively. All sequences in boldface are n-length sequences, where $n \in \mathbb{N}^*$, unless specified otherwise. A sequence of random variables $(Y_j, Y_{j+1}, \ldots, Y_k)$ is denoted by $\mathbf{Y}_j^k$. We drop the subscript and superscript when the context is clear. The element at position $\ell \in [\![1, n]\!]$ of a sequence $\mathbf{x}_j$ is denoted by $x_{j,\ell}$. Throughout this document, we interpret log and exp to the base 2. Adhering to standard information-theoretic notation, $\mathbb{H}(X)$ represents the average entropy of X. For $p \in [0, 1]$, let $\mathbb{H}_b(p)$ represent the binary entropy: $\mathbb{H}_b(p) \triangleq -p \log p - (1-p) \log(1-p)$. If the distribution of X and the channel between X and Y are represented by P and $W_{Y|X}$, respectively, both $\mathbb{I}(X;Y)$ and $\mathbb{I}\big(P, W_{Y|X}\big)$ represent the average mutual information between X

[4] in some cases, covert communication can be achieved without a secret key.

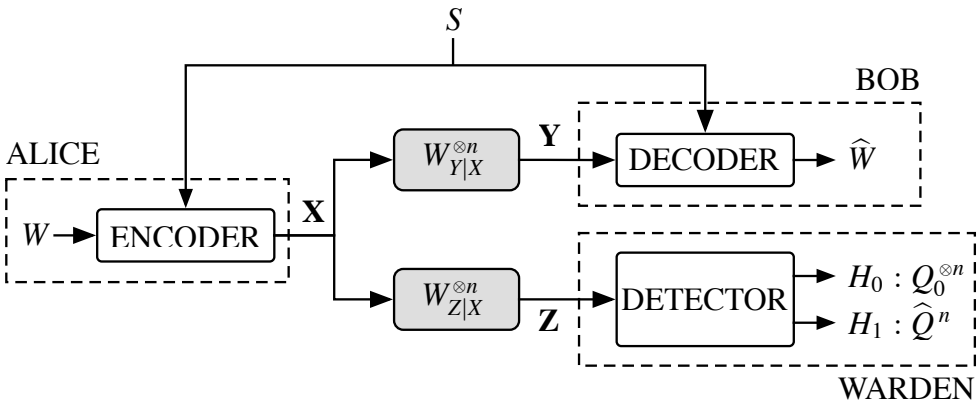

Figure 2.3: Covert communication over a point-to-point channel.

and Y. For two distributions, P and Q, defined on the same finite alphabet $\mathcal{X}$, the Kullback-Leibler (KL) divergence is $\mathbb{D}(P\|Q) \triangleq \sum_x P(x) \log \frac{P(x)}{Q(x)}$ and the variational distance is $\mathbb{V}(P,Q) \triangleq \frac{1}{2}\sum_x |P(x) - Q(x)|$. KL divergence and variational distance are related by Pinsker's inequality [26] as $\mathbb{V}(P,Q)^2 \leqslant \frac{1}{2}\mathbb{D}(P\|Q)$. We denote the *chi-squared* distance between two distributions P and Q by $\chi(P\|Q) \triangleq \sum_x \frac{(P(x)-Q(x))^2}{Q(x)}$. If P is absolutely continuous with respect to (w.r.t.) Q, we write $P \ll Q$. For $x \in \mathbb{R}$, we define $[x]^+ \triangleq \max(x, 0)$. For a set $\mathcal{T}$, we represent the vector $\{X_k : k \in \mathcal{T}\}$ by $X[\mathcal{T}]$. We denote the cartesian product $\times_{k\in\mathcal{T}}\mathcal{X}_k$ by $\mathcal{X}[\mathcal{T}]$ and an empty set by $\emptyset$, the cardinality of a set $\mathcal{T}$ by $|\mathcal{T}|$, and the set difference of two sets $\mathcal{S}$ and $\mathcal{T}$ by $\mathcal{S} \setminus \mathcal{T}$.

2.2.2 Information-theoretic framework for LPD communication

To set up a mathematical framework for LPD communication, we use the point-to-point channel model [27] illustrated in Figure 2.3, in which Alice, the legitimate transmitter, transmits a covert message W to Bob, the legitimate receiver, using a secret key S while simultaneously escaping detection from Willie, the warden. Alice encodes a uniformly distributed message $W \in [\![1, M]\!]$ and a uniformly distributed secret key $S \in [\![1, K]\!]$ into an n-length codeword $\mathbf{X}(W,S) \in \mathcal{X}^n$ and transmits over the Discrete Memoryless Channel (DMC) $\left(\mathcal{X}, W_{Y|X}, \mathcal{Y}\right)$ in the presence of Willie who monitors the communication over another DMC $\left(\mathcal{X}, W_{Z|X}, \mathcal{Z}\right)$. Bob observes

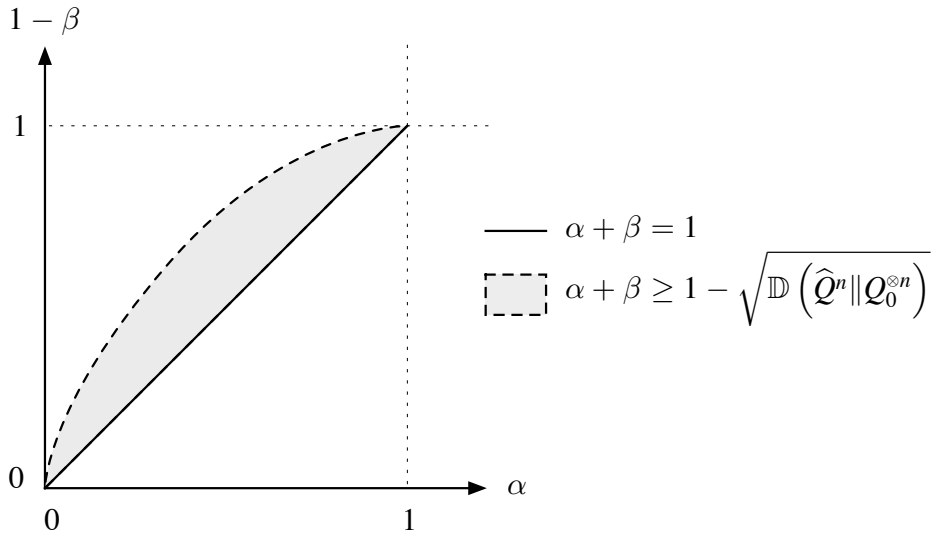

Figure 2.4: ROC curve of Willie's detector

$\mathbf{Y} \in \mathcal{Y}^n$ and forms an estimate $\widehat{W}$ of W with knowledge of the key S, whereas Willie observes $\mathbf{Z} \in \mathcal{Z}^n$ and performs a hypothesis test that we explain later. Since the channel to Willie is memoryless, we define the transition probability corresponding to n uses of the channel by $W_{Z|X}^{\otimes n} \triangleq \prod_{i=1}^{n} W_{Z|X}$. We assume a binary-input alphabet $\mathcal{X} \triangleq \{0, 1\}$ and finite output alphabets $\mathcal{Y}$ and $\mathcal{Z}$. We let $0 \in \mathcal{X}$ be the innocent symbol corresponding to the channel input when no communication takes place.

2.2.3 Hypothesis testing

In the channel model detailed above, the primary objective of Willie is to detect whether Alice transmits a covert message or not based on his observation $\mathbf{Z}$. Towards that end, Willie performs a statistical hypothesis test on his observation $\mathbf{Z}$, with the null hypothesis H_0 corresponding to the absence of any covert transmission and the alternate hypothesis H_1 corresponding to the presence of a covert transmission. During this process, Willie might make two types of errors, namely, the *probability of false alarm* defined by $\alpha \triangleq \mathbb{P}(H_1 \text{ is accepted} | H_0 \text{ is true})$ and the *probability of missed detection* defined by $\beta \triangleq \mathbb{P}(H_0 \text{ is accepted} | H_1 \text{ is true})$. While β is a measure of Alice's ability to evade detection, α is a measure of how certain Willie is that he has detected

a covert transmission. To illustrate the performance of Willie's detector, we plot its Receiver Operating Characteristic (ROC) curve, which is a plot of the probability of detection $(1-\beta)$ against the probability of false alarm α, in Figure 2.4. Ideally, Willie would want to operate at the point $(0,1)$, where he can detect any transmission without any error making transmission of covert messages impossible. On the other hand, if Willie ignores his observation and bases his decision on the result of a random coin-toss, he can operate at any point on the diagonal on which $\alpha+\beta=1$, and it corresponds to his worst performance in detecting the covert transmission.

Defining $Q_0^{\otimes n}(\mathbf{z}) \triangleq \prod_{i=1}^{n} Q_0(z_i)$, where $Q_0(z) \triangleq W_{Z|X}(z|0)$, we let $Q_0^{\otimes n}$ be the innocent distribution expected at Willie when no covert communication takes place. We also define $\widehat{Q}^n$ as the distribution induced at Willie by covert transmission. Willie then constructs an optimal hypothesis test that minimizes $\alpha+\beta$ to attribute his observation $\mathbf{Z}$ to either $Q_0^{\otimes n}$ or $\widehat{Q}^n$. According to [28], for any hypothesis test, $\alpha+\beta \geqslant 1-\mathbb{V}\left(\widehat{Q}^n, Q_0^{\otimes n}\right)$. Using Pinsker's inequality, we write $\alpha+\beta \geqslant 1-\sqrt{\mathbb{D}\left(\widehat{Q}^n \| Q_0^{\otimes n}\right)}$. Since our objective is to escape detection from Willie, we want the decision of the statistical test used by Willie to be no better than a random guess, *i.e.*, we want to restrict Willie to operating close to the diagonal. Bloch [27] provided an alternate operational significance of $\mathbb{D}\left(\widehat{Q}^n \| Q_0^{\otimes n}\right)$ using the *Jensen-Shannon divergence* and showed that a sufficient condition to make the test ineffective is to make $\mathbb{D}\left(\widehat{Q}^n \| Q_0^{\otimes n}\right)$ negligible, which in turn guarantees that Willie's detector operates close to the diagonal. Note that we only constrain Willie to operate close to the diagonal; the exact point of operation of the detector is determined by Willie. In [29], Tahmasbi and Bloch used each of the following metrics to measure covertness — KL divergence, variational distance, and the optimal probability of missed detection for a fixed α — and showed that measuring covertness in terms of the variational distance captures the operational performance of Willie better than using KL divergence or the optimal β for a fixed α. However, throughout this document, we use the KL divergence as our covertness

metric for reasons that we discuss in Section 2.3.1.

2.2.4 Previous works on LPD communication

In this subsection, we summarize previous works related to LPD communication. Inspired by steganographic techniques and Hero's secure space-time codes [30], Bash *et al.* [25] analyzed covert communication[5], over a point-to-point channel model obtained by replacing the DMCs in Figure 2.3 with Additive White Gaussian Noise (AWGN) channels. They showed that covert communication is subject to the *square-root law*, which states that Alice can only send $\mathcal{O}(\sqrt{n})$ bits to Bob in n channel uses while ensuring that $\alpha + \beta \geqslant 1 - \epsilon$ for an arbitrary $\epsilon > 0$ at Willie. Alternatively, transmitting $\omega(\sqrt{n})$ bits in n channel uses either results in detection by Willie with probability one or a non-zero decoding error probability at Bob as $n \to \infty$ [25]. The square-root law for LPD communication schemes [31] stems from the observation that the standard deviation of the noise distribution over n channel uses is on the order of $\mathcal{O}(\sqrt{n})$, and Alice employs a per-symbol transmit power of $\mathcal{O}\left(\frac{1}{\sqrt{n}}\right)$ to induce a distribution that is indistinguishable from the one induced by just noise from the perspective of Willie. Moreover, the square-root law translates to zero rate since $\lim_{n\to\infty} \frac{\mathcal{O}(\sqrt{n})}{n} = 0$, *i.e.*, the ratio of the number of bits transmitted to the number of channel uses vanishes asymptotically. Although Hero [30] first identified that an LPD communication scheme is subject to an average power constraint, he did not analyze the constraint asymptotically. As a result, he did not observe the square-root law first identified in steganography.

In the scheme analyzed by Bash *et al.* [25], Alice randomly chooses $\mathcal{O}(\sqrt{n})$ embedding locations out of n symbols and shares this set of locations with Bob. Each symbol location is represented by $\log n$ bits and there are $\mathcal{O}(\sqrt{n})$ such symbol locations. Hence, a secret key of size $\mathcal{O}(\sqrt{n}\log n)$ has to be shared between Alice and Bob

[5]Henceforth, we use covert communication as an alias for LPD communication.

prior transmission. This scheme is rather inefficient since the key is longer than the actual message to be hidden. Surprisingly, Che *et al.* [32] showed that a secret key is unnecessary for covert communication over a Binary Symmetric Channel (BSC) provided the channel to the warden is noisier than the channel to the legitimate receiver. Later, Bloch [27] generalized the results to DMCs and showed that the size of the shared key can be reduced from $\mathcal{O}\left(\sqrt{n}\log n\right)$ to $\mathcal{O}\left(\sqrt{n}\right)$ bits using channel resolvability techniques, which we discuss later in this section. Following the idea that the use of a secret key can be avoided if Bob can exploit a channel asymmetry to his advantage, Bloch also formulated the channel condition required for keyless covert communication [27]. Wang [33] developed a converse for the square-root law, which when combined with the achievable scheme outlined in [27], established a tight first-order asymptotic characterization of the covert throughput over point-to-point channels. Subsequently, Tahmasbi and Bloch [29] analyzed the second-order asymptotic characterization of the covert throughput. Tahmasbi *et al.* [34] also developed upper and lower bounds for the error exponent of covert communication over binary-input DMCs.

It is important to note that while covertness ensures that the presence of a covert message is hidden from the warden, he is not forbidden from trying to decode his observation. However, in certain scenarios, legitimate users might want to keep the transmission secret in addition to hiding it. Towards that end, Bloch [27] showed that under certain channel conditions, a portion of the covert message is inherently secret from the warden and that the transmitter can secure the remaining portion of the message by using a secret key. In [35, 36], the authors require their covert communication schemes to be *hidable* in addition to being covert, *i.e.*, the warden should not be able to estimate what the potential message is, even if he assumes the presence of a covert message. They showed that the transmitter can still send $\mathcal{O}\left(\sqrt{n}\right)$ covert bits despite the additional hidability requirement.

While instituting a channel asymmetry in favor of the receiver can help transmit $\mathcal{O}(\sqrt{n})$ covert bits without the need for a secret key, the uncertainty of the warden about channel noise parameters helps the users transmit a linear number of covert bits in some cases. In case the warden is uncertain about the BSC noise parameter, Che *et al.* [37] showed that the square-root law can be circumvented even if an impairing assumption that the receiver is also uncertain about his channel noise parameter is made. Lee *et al.* [38, 39] investigated LPD communication in AWGN Rayleigh channels with noise uncertainty at the warden and a sub-optimal radiometer at his disposal, and affirmed that if Alice transmits below the SNR wall [40], which is the threshold below which the detector is non-robust, it is impossible for the warden to detect covert transmission even if the rate is linear. Moreover, Lee *et al.* [41] extended their techniques over Multiple-Input Multiple-Output (MIMO) Rayleigh channels and quantified the improvement in covert throughput as a result of increasing the number of antennas at the legitimate users. Alternatively, Lee *et al.* [42] established channel asymmetry in a state-dependent AWGN channel by letting the transmitter possess non-causal channel state information and showed that covert bits can be transmitted with a linear rate.

It is common practice in information-theoretic works to assume that all users involved are synchronized, *i.e.*, all users are aware of the start and end times of the transmission. However, in covert communication scenarios, in which the transmitter tries to hide his presence in the network, it is justified to assume that warden is not synchronized with the transmitter. It is also fair to assume that the legitimate users are still synchronized since they can use a part of their secret key to synchronize before transmission. Since the warden is unaware of the start time of the transmission, he has to monitor the channel for a much longer duration than the actual transmission window. Bash *et al.* [43] showed that the transmitter can take advantage of this situation and transmit $\mathcal{O}\left(\min\left\{\sqrt{n\log T(n)}, n\right\}\right)$ bits to the receiver by choosing

a single slot of n symbols from $T(n)$ such slots. Although [43] requires a secret key denoting the index of the chosen time slot to be shared with the receiver, an additional key of size $\log T(n)$ results in a multiplicative gain of $\sqrt{\log T(n)}$ in the covert throughput. Subsequently, Goeckel *et al.* [44] proved an alternative result that the warden can restrict the transmitter to $\mathcal{O}\left(\min\left\{\sqrt{n\log T(n)}, n\right\}\right)$ covert bits in a similar channel setting even if he is uncertain about the background noise power. The result is attributed to the fact that the warden can learn the channel noise statistics from his observations since most of the time slots are unoccupied by the transmitter.

A few works have also attempted to transmit covert information in queues [45] by manipulating the timing between packets. Soltani *et al.* [46] analyzed a scheme that embeds covert information in the arrival times of packets in a Poisson packet channel. They showed that the transmitter can send $\mathcal{O}\left(\sqrt{\lambda T}\right)$ bits in time period T over an $M/M/1$ queue with arrival rate λ by inserting new packets into the channel and $\mathcal{O}\left(\lambda T\right)$ bits by altering the timing of incoming packets. Mukherjee and Ulukus [47] showed that one can achieve a positive rate by embedding covert information in the packet timings in exponential and general queues provided a high-rate secret key is available. Soltani *et al.* [48] also showed that covert bit insertion in packets whose sizes satisfy certain requirements are subject to the square-root law as well.

Since covert messages are hidden in noise, cooperative jammers can help the transmitter improve the covert rate via two methods. First, by generating background chatter, the jammers increase background noise and inhibit the warden's ability to detect covert transmission. Soltani *et al.* [49] quantified the improvement in covert throughput when a friendly jammer, who is proximally located to the warden, generates artificial noise. Second, by varying their transmit powers sufficiently, the jammers render the warden's observations outside the sender's transmission window futile in learning the statistics of the channel. However, these cooperative jammers should not be concerned to transmit non-covertly in the presence of the warden. In

the presence of non-covert cooperative nodes, the transmitter can route [50] covert information through them while ensuring that no communication between any two nodes in the multi-hop path is detected by the warden or multiple collaborating wardens.

Some works have also investigated explicit code constructions for covert communication. While low-complexity encoding and decoding is a crucial requirement for codes in general, codes for covert communication also need to be of low-weight and the information bits have to be spread out in the codeword to escape detection at the warden. Zhang *et al.* [51] constructed a computationally efficient coding scheme for BSC with an inner random code and an outer Reed-Solomon code. Addressing the sparsity requirement of covert codewords using Pulse Position Modulation (PPM)-based codes, Bloch and Guha [52] showed their optimality for covert communication over DMCs. Meanwhile, Frèche *et al.* [53] introduced a polarization-based code construction for asynchronous covert communication. Although polarization ensures low complexity, this particular coding scheme does not achieve covert capacity. Subsequently, Kadampot *et al.* [54] proved that linear codes cannot achieve covert capacity and devised a low complexity multi-level PPM-based coding scheme for binary-input DMCs that achieves covert capacity.

As discussed earlier, in certain scenarios, the users need access to a secret key to communicate covertly. However, it is possible that the users had not agreed upon a secret key earlier. In such scenarios, it is essential that the users synthesize a secret key covertly since a public attempt at key generation would result in the warden speculating a potential covert transmission. To this end, Tahmasbi and Bloch [55, 56] proposed a key distribution scheme in which the process itself is covert from the adversary.

Besides classical communication channels, an extensive body of literature also exists for covert communication over quantum channels. Bash *et al.* [57, 58] showed

that covert communication over a lossy thermal-noise bosonic channel is also subject to the square-root law. Sheikholeslami *et al.* [59] showed that classical-quantum channels are subject to the square-root law, while Wang [60] computed the exact optimal constant of the scaling.

2.2.5 Distinction from steganography

Unlike LPD communication schemes in which the transmitter only possesses knowledge of the statistical properties of the noise in which he attempts to hide his message, the steganographic transmitter possesses complete knowledge of the exact covertext before he embeds his message. Consequently, steganographic techniques are not necessarily robust against addition of noise from external sources. Since in LPD communication, the noise added by the channel serves as the cover in which the message is hidden, steganographic methods cannot be directly applied to communicate information across a noisy channel with LPD.

2.2.6 Distinction from stealth

Borrowing terminology from [61], we define communication schemes that shape message-carrying signals to resemble an innocent signal (as opposed to noise) as *stealth* or Low Probability of Interception (LPI) communication techniques. Essentially, LPI communication schemes attempt to prevent the adversary from analyzing the transmission to determine if it contains meaningful information or not. Although the definitions of LPD and LPI are deceptively similar, it is important to highlight the differences between them. First, LPD communication is an extreme version of LPI since the signals are shaped to hide in noise. Second, while the throughput in LPD communication is subject to the square-root law, LPI communication techniques achieve a positive rate by transmitting random codewords that approximate the target distribution at the receiver even if there is no transmission of information. In short,

LPD communication schemes attempt to approximate the innocent distribution $Q_0^{\otimes n}$, where $Q_0 = W_{Z|X}(z|0)$, whereas LPI communication schemes, for instance, attempt to approximate a target i.i.d. distribution $Q_Z^{\otimes n}$ where $Q_Z(z) \triangleq \sum_x P_X(x)W_{Z|X}(z|x)$ at the warden for some input distribution P_X [62].

2.3 Covert capacity

In this section, we introduce two concepts, namely, covert process and channel resolvability, that are essential to define and understand covert capacity. Then, we recall the characterization of the covert capacity [27] for the point-to-point channel illustrated in Figure 2.3.

2.3.1 Covert process

We introduce the notion of *covert process*, which is an i.i.d. process indistinguishable from the innocent distribution $Q_0^{\otimes n}$ in the limit. The rationale behind introducing the covert process is to precisely quantify the fraction of channel uses Alice can transmit symbol 1 while simultaneously avoiding detection from Willie. For $n \in \mathbb{N}^*$, we let $\alpha_n \in (0, 1)$. Let us define the input distribution Π_{α_n} on $\mathcal{X}$ by

$$\Pi_{\alpha_n}(1) = 1 - \Pi_{\alpha_n}(0) = \alpha_n. \tag{2.1}$$

Define the output distribution at Willie by

$$Q_{\alpha_n}(z) \triangleq \sum_x \Pi_{\alpha_n}(x)W_{Z|X}(z|x). \tag{2.2}$$

We represent the n-fold product distributions corresponding to (2.1) and (2.2) by

$$\Pi_{\alpha_n}^{\otimes n} = \prod_{i=1}^{n} \Pi_{\alpha_n}, \quad Q_{\alpha_n}^{\otimes n} = \prod_{i=1}^{n} Q_{\alpha_n}. \tag{2.3}$$

Lemma 1. *[27, Lemma 1] Let* $\{\alpha_n\}_{n\geqslant 1}$ *be such that* $\alpha_n \in (0, 1)$ *and* $\lim_{n\to\infty} \alpha_n = 0$.

Then, for $n \in \mathbb{N}^*$ large enough,

$$\frac{\alpha_n^2}{2}\left(1+\sqrt{\alpha_n}\right)\chi\left(Q_1\|Q_0\right) \geqslant \mathbb{D}(Q_{\alpha_n}\|Q_0) \geqslant \frac{\alpha_n^2}{2}\left(1-\sqrt{\alpha_n}\right)\chi\left(Q_1\|Q_0\right). \tag{2.4}$$

If Alice generates an n-length sequence $\mathbf{x}$ using the product distribution $\Pi_{\alpha_n}^{\otimes n}$, the weight of $\mathbf{x}$ is $n\alpha_n$ on average. Moreover, for the covert process to be indistinguishable from $Q_0^{\otimes n}$ in the limit, $Q_{\alpha_n}^{\otimes n}$ has to satisfy

$$\lim_{n\to\infty} \mathbb{D}\big(Q_{\alpha_n}^{\otimes n}\|Q_0^{\otimes n}\big) = \lim_{n\to\infty} n\mathbb{D}(Q_{\alpha_n}\|Q_0) = 0. \tag{2.5}$$

Using KL divergence instead of variational distance as our covertness metric allows us to write (2.5) by taking advantage of the i.i.d. property of $Q_{\alpha_n}^{\otimes n}$ and $Q_0^{\otimes n}$, and enables us to use the results of Lemma 1 to conclude that if we choose the sequence $\{\alpha_n\}_{n\in\mathbb{N}^*}$ such that $\lim_{n\to\infty} n\alpha_n^2 = 0$, then Willie cannot distinguish between $Q_{\alpha_n}^{\otimes n}$ and $Q_0^{\otimes n}$ in the limit. Hence, the process $Q_{\alpha_n}^{\otimes n}$ is covert if the input parameter α_n is on the order of $\frac{1}{\sqrt{n}}$. As a consequence, the input sequence generated by $\Pi_{\alpha_n}^{\otimes n}$ has $\sqrt{n}$ information symbols on average confirming that the rate of covert transmission is subject to the square-root law.

By definition, for LPD communication, we wish to design a scheme that induces a distribution close to $Q_0^{\otimes n}$. We have already proved that the process $Q_{\alpha_n}^{\otimes n}$ and $Q_0^{\otimes n}$ are indistinguishable in the limit. Alternatively, designing a scheme that approximates $Q_{\alpha_n}^{\otimes n}$ instead of $Q_0^{\otimes n}$ allows us to convey covert information by using symbol 1. Specifically, we can choose the sequence $\{\alpha_n\}_{n\in\mathbb{N}^*}$ such that $\lim_{n\to\infty} n\alpha_n = \infty$ so that the number of information bits grows as n grows to infinity, thus conveying covert information. To design a communication scheme that induces a distribution close to the covert process $Q_{\alpha_n}^{\otimes n}$, we use channel resolvability techniques, which we discuss next.

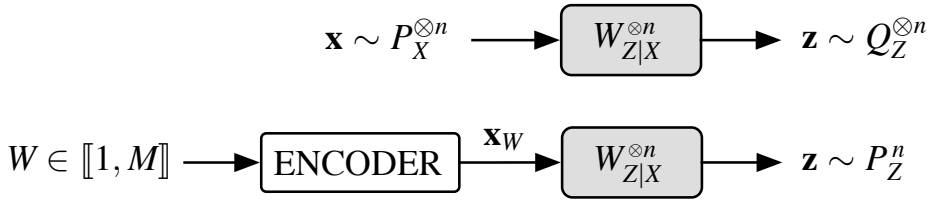

Figure 2.5: Approximation of output statistics

2.3.2 Channel resolvability

To explain the notion of channel resolvability first introduced by Han and Verdú [63], we consider the channel model illustrated in Figure 2.5. In the first instance shown at the top part of the figure, transmitting an n-length i.i.d. input sequence $\mathbf{X} \triangleq (X_1, X_2, \ldots, X_n)$ distributed according to $P_X^{\otimes n}$ through the DMC $\left(\mathcal{X}, W_{Y|X}, \mathcal{Y}\right)$ induces an i.i.d. output sequence $\mathbf{Z} \triangleq (Z_1, Z_2, \ldots, Z_n)$ distributed according to $Q_Z^{\otimes n}$.

$$Q_Z^{\otimes n}(\mathbf{z}) \triangleq \sum_{\mathbf{x}} W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{x}) P_X^{\otimes n}(\mathbf{x}). \tag{2.6}$$

As shown in the second instance at the bottom part of Figure 2.5, we wish to approximate the output distribution $Q_Z^{\otimes n}$ using a set of M codewords $\{\mathbf{x}_w\}_{w=1}^M$ generated according to the distribution $P_X^{\otimes n}$. Let us denote the distribution induced by the codewords $\{\mathbf{x}_w\}_{w=1}^M$ at the output by

$$P_Z^n \triangleq \frac{1}{M} \sum_{w=1}^{M} W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{x}_w). \tag{2.7}$$

Then, we can guarantee [63] that there exist codebooks with $\lim_{n\to\infty} \mathbb{D}(P_Z^n \| Q_Z^{\otimes n}) = 0$ if $\log M > \mathbb{I}(X;Y)$. Intuitively, transmitting at a rate above the capacity of the channel $W_{Z|X}$ causes the transmission to lose all of its structure at the output and results in an output distribution that closely approximates the reference distribution. The minimum of all achievable resolvability rates over the channel $W_{Z|X}$ w.r.t. the reference distribution Q_Z is called the resolvability of the channel $W_{Z|X}$. This set of

codewords $\{\mathbf{x}_w\}_{m=1}^{M}$ forms a channel resolvability code for the channel $W_{Z|X}$ w.r.t. the distribution $Q_Z^{\otimes n}$.

For LPD communication, channel resolvability codes are especially useful to approximate the covert process $Q_{\alpha_n}^{\otimes n}$ at Willie. If our codebook $\mathcal{C}$ induces an output distribution $\widehat{Q}^n$, the codebook $\mathcal{C}$ is a channel resolvability code that approximates the covert process $Q_{\alpha_n}^{\otimes n}$ at the warden if $\lim_{n\to\infty} \mathbb{D}\Big(\widehat{Q}^n \| Q_{\alpha_n}^{\otimes n}\Big) = 0$. Bloch [27] first used channel resolvability-based codes for LPD and showed that they can achieve covert capacity over a point-to-point channel. In all subsequent chapters, we use channel resolvability-based codes in our covert communication schemes.

2.3.3 Covert capacity of a point-to-point channel

For the channel model illustrated in Figure 2.3, Alice needs to ensure that her communication is both reliable at Bob and undetectable at Willie, *i.e.*, $\lim_{n\to\infty} \mathbb{P}\Big(\widehat{W} \neq W\Big) = 0$ and $\lim_{n\to\infty} \mathbb{D}\Big(\widehat{Q}^n \| Q_0^{\otimes n}\Big) = 0$. Consequently, covert communication falls in the zero-rate regime in which the number of covert bits scales sub-linearly with the number of channel uses. Hence, it is necessary to normalize $\log M$ differently to characterize the number of covert bits that can be transmitted in n channel uses. Combining the fact that $\log M$ is subject to the square-root law and the fact that $\mathbb{D}\Big(\widehat{Q}^n \| Q_0^{\otimes n}\Big)$ influences $\log M$, we normalize it by $\sqrt{n\mathbb{D}\Big(\widehat{Q}^n \| Q_0^{\otimes n}\Big)}$ to get meaningful constants as shown in the following theorem. Note that we refer to $\frac{\log M^*}{\sqrt{n\mathbb{D}\left(\widehat{Q}^n \| Q_0^{\otimes n}\right)}}$ as *throughput* rather than *rate* to emphasize the different normalization.

Theorem 1. *[27] For the point-to-point channel model illustrated in Figure 2.3 with $P_1 \ll P_0$, $Q_1 \ll Q_0$, and $Q_1 \neq Q_0$, define*

$$\chi\left(Q_1 \| Q_0\right) \triangleq \sum_z \frac{\left(Q_1(z) - Q_0(z)\right)^2}{Q_0(z)}. \tag{2.8}$$

Let M^* be the largest possible value of M such that a code with increasing block length

n can be constructed to satisfy $\lim_{n\to\infty} \mathbb{D}\left(\widehat{Q}^n \| Q_0^{\otimes n}\right) = 0$ *and* $\lim_{n\to\infty} \mathbb{P}\left(\widehat{W} \neq W\right) = 0$. *Then, the covert capacity of the point-to-point channel is*

$$\lim_{n\to\infty} \frac{\log M^*}{\sqrt{n\mathbb{D}\left(\widehat{Q}^n \| Q_0^{\otimes n}\right)}} = \sqrt{\frac{2}{\chi\left(Q_1 \| Q_0\right)}} \mathbb{D}(P_1 \| P_0). \tag{2.9}$$

In addition, to achieve a covert throughput that matches the covert capacity, the achievable key throughput has to satisfy

$$\lim_{n\to\infty} \frac{\log K}{\sqrt{n\mathbb{D}\left(\widehat{Q}^n \| Q_0^{\otimes n}\right)}} \geqslant \sqrt{\frac{2}{\chi\left(Q_1 \| Q_0\right)}} \left[\mathbb{D}(Q_1 \| Q_0) - \mathbb{D}(P_1 \| P_0)\right]^+. \tag{2.10}$$

In the achievability proof, Bloch [27] used channel resolvability-based codes to first approximate the covert process $Q_{\alpha_n}^{\otimes n}$ defined in (2.3). Then, using the result of Lemma 1, he proves that the proposed communication scheme is indeed covert. From Theorem 1, we conclude that Alice can achieve her maximum covert throughput without a secret key only if $\mathbb{D}(P_1 \| P_0) \geqslant \mathbb{D}(Q_1 \| Q_0)$, *i.e.*, if the channel from Alice to Bob is *better* than the channel from Alice to Willie.

CHAPTER 3
COVERT COMMUNICATION OVER A K-USER MULTIPLE-ACCESS CHANNEL

3.1 Summary

In this chapter, we consider a scenario in which K transmitters attempt to communicate covert messages reliably to a legitimate receiver over a discrete memoryless MAC while simultaneously escaping detection from an adversary who observes their communication through another discrete memoryless MAC. We assume that each transmitter may use a secret key that is shared only between itself and the legitimate receiver. We show that each of the K transmitters can transmit on the order of $\sqrt{n}$ reliable and covert bits per n channel uses, exceeding which, the warden will be able to detect the communication. We identify the optimal pre-constants of the scaling, which leads to a complete characterization of the covert capacity region of the K-user binary-input MAC. We show that, asymptotically, all sum-rate constraints are inactive unlike the traditional MAC capacity region. We also characterize the channel conditions that have to be satisfied for the transmitters to operate without a secret key.

3.2 Introduction

The main result developed in this paper is the characterization of the covert capacity region of the K-user binary-input MAC. The tools used are natural extensions of the techniques developed for point-to-point covert and stealth channels in [27, 33, 62] and for MAC resolvability [64, 65, 66], but the converse proof requires special care beyond the approach used in [27]. We show that, asymptotically, there exist no

sum-rate constraints unlike the traditional MAC rate region; intuitively, this happens because covertness is such a stringent constraint that the covert users never transmit enough bits to saturate the capacity of the channel. The system behaves as if a covert communication *budget* were merely allocated to the different users.[1] A similar behavior was observed [67, Theorem 6] in the calculation of the channel capacity per unit cost of a two-user MAC when both users consist of a *free* input symbol; however, note that the covert constraint is more stringent than an average per symbol cost constraint.

The remainder of this chapter is organized as follows. In Section 3.3, we formally introduce our channel model and define the covert capacity region. In Section 3.4, we develop a preliminary result that captures the essence of our approach to covertness and extends [27, Lemma 1]. We establish the covert capacity region of the K-user binary-input MAC in Section 3.5 and conclude our work with a brief discussion of extensions and open problems in Section 3.6. The proofs of all lemmas are relegated to the appendix at the end of this chapter. This chapter is based on the results obtained in [68, 69].

3.3 Channel model

We define the set $\mathcal{K} \triangleq [\![1, K]\!]$, where $K \in \mathbb{N}^*$ and $K \geqslant 2$. We analyze the channel model illustrated in Figure 3.1, in which K transmitters simultaneously communicate with a legitimate receiver over a discrete memoryless MAC $\left(\mathcal{X}[\mathcal{K}], W_{Y|X[\mathcal{K}]}, \mathcal{Y}\right)$ in the presence of a warden monitoring the communication over another discrete memoryless MAC $\left(\mathcal{X}[\mathcal{K}], W_{Z|X[\mathcal{K}]}, \mathcal{Z}\right)$. As both channels are memoryless, we denote the transition probabilities corresponding to n uses of the channel by $W_{Y|X[\mathcal{K}]}^{\otimes n} \triangleq \prod_{i=1}^{n} W_{Y|X[\mathcal{K}]}$ and $W_{Z|X[\mathcal{K}]}^{\otimes n} \triangleq \prod_{i=1}^{n} W_{Z|X[\mathcal{K}]}$. In addition, we assume for simplicity of exposition that each user $k \in \mathcal{K}$ uses the same binary input alphabet $\mathcal{X}_k \triangleq \mathcal{X} \triangleq \{0, 1\}$ and that the output

[1] This intuitive interpretation is attributed to Sidharth Jaggi, during discussions at ISIT 2016.

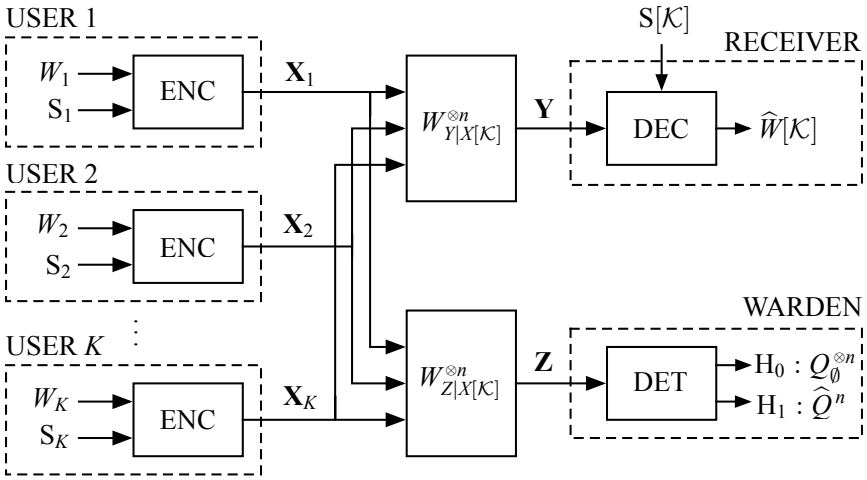

Figure 3.1: Model of covert communication over a MAC with K transmitters.

alphabets $\mathcal{Y}$ and $\mathcal{Z}$ are finite. We let $0 \in \mathcal{X}$ be the innocent symbol corresponding to the channel input when no communication takes place. We assume that all terminals are synchronized and possess complete knowledge of the coding scheme used.

The user indexed by $k \in \mathcal{K}$, encodes a uniformly-distributed message $W_k \in [\![1, M_k]\!]$ and a uniformly-distributed secret key $S_k \in [\![1, L_k]\!]$, which is shared only with the receiver, into a codeword $\mathbf{X}_k(W_k, S_k) \in \mathcal{X}^n$ of length n. We denote the collection of the K codewords $\{\mathbf{X}_k(W_k, S_k)\}_{k\in\mathcal{K}}$ by $\mathbf{X}_{\mathcal{K}}(W[\mathcal{K}], S[\mathcal{K}])$. When the context is clear, we drop the message and key indices, W_k and S_k, and denote $\mathbf{X}_k(W_k, S_k)$ by $\mathbf{X}_k$ instead for conciseness. It is convenient to think about the K inputs to the channel over n uses as a matrix $\mathbf{X}[\mathcal{K}]$ of size $K \times n$ obtained by vertically stacking the K codewords, each of which is a row vector. The inputs corresponding to all users indexed by the elements of a non-empty set $\mathcal{U} \subset \mathcal{K}$ is a sub-matrix of $\mathbf{X}[\mathcal{K}]$ obtained by selecting the rows whose indices belong to $\mathcal{U}$ and is denoted by $\mathbf{X}[\mathcal{U}]$. The K users then transmit codewords $\mathbf{X}[\mathcal{K}]$ over the channel in n channel uses. At the end of transmission, the receiver observes $\mathbf{Y}$ while the warden observes $\mathbf{Z}$, both of which are of length n.

We introduce a K-length row vector $X_{\mathcal{U}} = (X_1, X_2, \ldots, X_K)$, $\mathcal{U} \subseteq \mathcal{K}$, with entry $X_k = 1$ if $k \in \mathcal{U}$ and $X_k = 0$ otherwise. With our assumption that all channel inputs

are binary, we represent every column of the matrix $\mathbf{X}[\mathcal{K}]$ by a vector $(X_{\mathcal{U}})^T$, where the set $\mathcal{U}$ consists of the indices of all users transmitting symbol 1 in this column. We denote the k^{th} component of $X_{\mathcal{U}}$ by $X_{\mathcal{U},k}$. In accordance with the notation introduced in the previous paragraph, $X_{\mathcal{U}}[\mathcal{T}]$ represents a row vector of length $|\mathcal{T}|$ that contains the entries $\{X_{\mathcal{U},k}\}_{k\in\mathcal{T}}$. Note the difference between $X[\mathcal{U}]$ and $X_{\mathcal{U}}$; the former is a $|\mathcal{U}|$-length vector $\{X_k\}_{k\in\mathcal{U}}$ whereas the latter is a K-length vector with 1's in indices that belong to the set $\mathcal{U}$. For conciseness, we define

$$P_{\mathcal{U}}(y) \triangleq W_{Y|X[\mathcal{K}]}(y|x_{\mathcal{U}}), \quad Q_{\mathcal{U}}(z) \triangleq W_{Z|X[\mathcal{K}]}(z|x_{\mathcal{U}}), \tag{3.1}$$

which represent the one-shot output distributions at the legitimate receiver and the warden, respectively, when only the transmitters in $\mathcal{U} \subseteq \mathcal{K}$ transmit symbol 1, while the transmitters in $\mathcal{U}^c$ transmit a 0. When $\mathcal{U}$ is a singleton set $\{k\}$, which corresponds to user k transmitting 1 and all other users transmitting 0, we write P_k and Q_k instead of $P_{\{k\}}$ and $Q_{\{k\}}$, respectively. If $\mathcal{U} = \emptyset$, which occurs when all users transmit the innocent symbol 0, we write $P_\emptyset$ and $Q_\emptyset$. We assume that $Q_{\mathcal{U}} \ll Q_\emptyset$ for all non-empty sets $\mathcal{U} \subseteq \mathcal{K}$ and that $Q_\emptyset$ cannot be written as a convex combination of the form $Q_\emptyset(z) = \sum_{\mathcal{T}\subseteq\mathcal{K}} \left(\prod_{k\in\mathcal{T}} \mu_k\right) \left(\prod_{k\in\mathcal{T}^c}(1-\mu_k)\right) Q_{\mathcal{T}}(z)$ for some $\{\mu_k\}_{k\in\mathcal{K}} \in [0,1]^K \setminus \{0\}_{k\in\mathcal{K}}$. In the former case, covert communication involving all K users is impossible; in the latter case, covert communication would directly follow from known channel resolvability results [64, 65, 66] and would be possible at a non zero-rate. We also assume that there does not exist $\{\rho_k\}_{k\in\mathcal{K}} \in [0,1]^K$ with $\sum_{k\in\mathcal{K}} \rho_k = 1$ such that $\sum_{k\in\mathcal{K}} \rho_k Q_k(z) = Q_\emptyset(z)$ for all $z \in \mathcal{Z}$. As we shall see later in Section 3.4, the square root law of covert communication can be circumvented if such a $\{\rho_k\}_{k\in\mathcal{K}}$ exists.

Upon observing $\mathbf{Y}$, the legitimate receiver estimates the message vector $\widehat{W}[\mathcal{K}]$. We measure reliability with the average probability of error $P_e^n \triangleq \mathbb{P}\left(\widehat{W}[\mathcal{K}] \neq W[\mathcal{K}]\right)$. Upon observing $\mathbf{Z}$, the warden attempts to detect whether all K users transmitted

covert messages (Hypothesis H_1) or not (Hypothesis H_0) by performing a hypothesis test on $\mathbf{Z}$. We denote the Type I (rejecting H_0 when true) and Type II (accepting H_0 when false) error probabilities by α and β, respectively. The warden can achieve any pair (α, β) such that $\alpha + \beta = 1$ by ignoring his observation $\mathbf{Z}$ and basing his decision on the result of a coin toss. We define the distribution induced at the warden when communication takes place by

$$\widehat{Q}^n(\mathbf{z}) \triangleq \frac{1}{\prod_{k\in\mathcal{K}} M_k L_k} \sum_{m[\mathcal{K}]} \sum_{\ell[\mathcal{K}]} W_{Z|X[\mathcal{K}]}^{\otimes n} \left(\mathbf{z}|\mathbf{x}_{\mathcal{K}}\left(m[\mathcal{K}], \ell[\mathcal{K}]\right)\right). \tag{3.2}$$

We measure covertness in terms of the KL divergence $\mathbb{D}\big(\widehat{Q}^n \| Q_{\emptyset}^{\otimes n}\big)$, where $Q_{\emptyset}^{\otimes n}$ is the distribution observed by the warden when none of the K users transmits any covert information. We know from [70] that any test conducted by the warden on $\mathbf{Z}$ satisfies $\alpha + \beta \geqslant 1 - \mathbb{V}\big(\widehat{Q}^n, Q_{\emptyset}^{\otimes n}\big)$. Using Pinsker's inequality [26], we write $\alpha + \beta \geqslant 1 - \sqrt{\mathbb{D}\big(\widehat{Q}^n \| Q_{\emptyset}^{\otimes n}\big)}$. The primary objective of our covert communication scheme is to guarantee that $\mathbb{D}\big(\widehat{Q}^n \| Q_{\emptyset}^{\otimes n}\big)$ is negligible so that any statistical test used by the warden on $\mathbf{Z}$ is futile.

Definition 1. *The tuple $r[\mathcal{K}] \in \mathbb{R}_+^K$ is an achievable reliable and covert throughput tuple*[2] *if there exists a sequence of codes as defined above with increasing blocklength n such that for every $k \in \mathcal{K}$,*

$$\liminf_{n\to\infty} \frac{\log M_k}{\sqrt{n\mathbb{D}\big(\widehat{Q}^n \| Q_{\emptyset}^{\otimes n}\big)}} \geqslant r_k, \tag{3.3}$$

and

$$\lim_{n\to\infty} P_e^n = 0, \quad \lim_{n\to\infty} \mathbb{D}\Big(\widehat{Q}^n \| Q_{\emptyset}^{\otimes n}\Big) = 0. \tag{3.4}$$

[2]We only consider communication schemes for which $\log M_k$ grows to infinity, for $k \in \mathcal{K}$, as n grows to infinity.

The covert capacity region of the K-user MAC consists of the closure of the set of all achievable throughput tuples $r[\mathcal{K}]$. A tuple $s[\mathcal{K}] \in \mathbb{R}_+^K$, associated to an achievable reliable and covert throughput tuple $r[\mathcal{K}]$, is an achievable key throughput tuple if for all $k \in \mathcal{K}$,

$$s_k \geqslant \limsup_{n\to\infty} \frac{\log L_k}{\sqrt{n\mathbb{D}\big(\widehat{Q}^n \| Q_\emptyset^{\otimes n}\big)}}. \tag{3.5}$$

Note that in (3.3), we normalize the number of bits $\log M_k$ by $\sqrt{n\mathbb{D}\big(\widehat{Q}^n \| Q_\emptyset^{\otimes n}\big)}$ instead of n as traditionally done in information-theoretic problems. The normalization by $\sqrt{n}$ is essential to reflect the fact that covert communication corresponds to a zero-rate regime, in which the number of bits scales sub-linearly with the number of channel uses. The normalization by $\sqrt{\mathbb{D}\big(\widehat{Q}^n \| Q_\emptyset^{\otimes n}\big)}$ is also crucial to reflect the fact that $\mathbb{D}\big(\widehat{Q}^n \| Q_\emptyset^{\otimes n}\big)$ influences $\{\log M_k\}_{k\in\mathcal{K}}$. While the normalization might seem somewhat ad-hoc, it is justified *a posteriori* in Section 3.5 when we prove that $\log M_k / \sqrt{n\mathbb{D}\big(\widehat{Q}^n \| Q_\emptyset^{\otimes n}\big)}$ is independent of n in the limit of large blocklength. Said differently, $\log M_k / \sqrt{n\mathbb{D}\big(\widehat{Q}^n \| Q_\emptyset^{\otimes n}\big)}$ plays the role of the usual "rate" in that it asymptotically does not depend on the blocklength n and already integrates the scaling. To avoid confusion, we refer to r_k as *throughput* instead of rate.

3.4 Preliminaries

Following the approach put forward in 2.3.1, we introduce a *covert communication process*, which is an i.i.d. process indistinguishable from the innocent distribution $Q_\emptyset^{\otimes n}$ in the limit. To recall, the rationale for introducing this process is to precisely quantify the fraction of channel uses in which the users can transmit symbol 1 while simultaneously avoiding detection by the warden, without introducing the coding aspect of the problem yet. For $n \in \mathbb{N}^*$, let $\alpha_n \in (0,1)$. Let $\boldsymbol{\rho} \triangleq \{\rho_k\}_{k\in\mathcal{K}} \in [0,1]^K$

such that[3] $\sum_{k\in\mathcal{K}}\rho_k = 1$. We define the input distributions $\{\Pi_{X_k}\}_{k\in\mathcal{K}}$ on $\mathcal{X}$ by

$$\Pi_{X_k}(1) = 1 - \Pi_{X_k}(0) = \rho_k\alpha_n. \tag{3.6}$$

The output distributions at the legitimate receiver and the warden when the input distribution of each user k is Π_{X_k} are defined, respectively, by

$$P_{\alpha_n}(y) \triangleq \sum_{x[\mathcal{K}]} W_{Y|X[\mathcal{K}]}(y|x[\mathcal{K}]) \left(\prod_{k\in\mathcal{K}} \Pi_{X_k}(x_k)\right), \tag{3.7}$$

$$Q_{\alpha_n}(z) \triangleq \sum_{x[\mathcal{K}]} W_{Z|X[\mathcal{K}]}(z|x[\mathcal{K}]) \left(\prod_{k\in\mathcal{K}} \Pi_{X_k}(x_k)\right). \tag{3.8}$$

The n-fold product distributions corresponding to (3.6), (3.7), and (3.8) are

$$\Pi_{X_k}^{\otimes n} = \prod_{j=1}^{n} \Pi_{X_k}, \quad P_{\alpha_n}^{\otimes n} = \prod_{j=1}^{n} P_{\alpha_n}, \quad Q_{\alpha_n}^{\otimes n} = \prod_{j=1}^{n} Q_{\alpha_n}. \tag{3.9}$$

For a set $\mathcal{T} \subseteq \mathcal{K}$, we define

$$G_{\mathcal{T}}(z) \triangleq \sum_{\mathcal{U}\subseteq\mathcal{T}} (-1)^{|\mathcal{T}|-|\mathcal{U}|} Q_{\mathcal{U}}(z). \tag{3.10}$$

Then, using Lemma 6 in Appendix 3.A, we write

$$Q_{\alpha_n}(z) = Q_{\emptyset}(z) + \sum_{\mathcal{T}\subseteq\mathcal{K}:\mathcal{T}\neq\emptyset} \left(\prod_{k\in\mathcal{T}} \rho_k\alpha_n\right) G_{\mathcal{T}}(z). \tag{3.11}$$

[3]The assumption $\sum_k \rho_k = 1$ is only made for convenience and, as we shall see from the converse part of Theorem 2, without loss of generality.

Note that since $Q_{\mathcal{T}} \ll Q_{\emptyset}$ for all non-empty sets $\mathcal{T} \subseteq \mathcal{K}$, it is also true that $Q_{\alpha_n} \ll Q_{\emptyset}$. Furthermore, we define

$$\zeta_n(z) \triangleq \frac{Q_{\alpha_n}(z) - Q_{\emptyset}(z)}{\alpha_n}, \quad \chi_n(\boldsymbol{\rho}) \triangleq \sum_z \frac{\zeta_n^2(z)}{Q_{\emptyset}(z)}, \tag{3.12}$$

$$\zeta(z) \triangleq \sum_{k \in \mathcal{K}} \rho_k (Q_k(z) - Q_{\emptyset}(z)), \quad \chi(\boldsymbol{\rho}) \triangleq \sum_z \frac{\zeta^2(z)}{Q_{\emptyset}(z)}. \tag{3.13}$$

In the following lemma, we bound the KL divergence between Q_{α_n} and $Q_{\emptyset}$. Later, we use the results of this lemma to show that for specific choices of the sequence $\{\alpha_n\}_{n \in \mathbb{N}^*}$, the stochastic process $Q_{\alpha_n}^{\otimes n}$ is indistinguishable from the innocent distribution $Q_{\emptyset}^{\otimes n}$ in the limit.

Lemma 2. *Let the sequence $\{\alpha_n\}_{n \geqslant 1}$ be such that $\lim_{n \to \infty} \alpha_n = 0$. Then, for $n \in \mathbb{N}^*$ large enough, we have*

$$\frac{\alpha_n^2}{2} \left(1 + \sqrt{\alpha_n}\right) \chi_n(\boldsymbol{\rho}) \geqslant \mathbb{D}(Q_{\alpha_n} \| Q_{\emptyset}) \geqslant \frac{\alpha_n^2}{2} \left(1 - \sqrt{\alpha_n}\right) \chi_n(\boldsymbol{\rho}). \tag{3.14}$$

In addition, for all $z \in \mathcal{Z}$, $\lim_{n \to \infty} \zeta_n(z) = \zeta(z)$ and $\lim_{n \to \infty} \chi_n(\boldsymbol{\rho}) = \chi(\boldsymbol{\rho})$. Finally, for random variables $(X[\mathcal{T}], Z) \in \mathcal{X}^{|\mathcal{T}|} \times \mathcal{Z}$ for some non-empty set $\mathcal{T} \subseteq \mathcal{K}$ with joint distribution $W_{Z|X[\mathcal{T}]} \left(\prod_{k \in \mathcal{T}} \Pi_{X_k}\right)$, we have

$$\mathbb{I}(X[\mathcal{T}]; Z) = \sum_{k \in \mathcal{T}} \rho_k \alpha_n \mathbb{D}(Q_k \| Q_{\emptyset}) + \mathcal{O}\left(\alpha_n^2\right). \tag{3.15}$$

The proof of Lemma 2 is provided in Appendix 3.B. Assume that each transmitter $k \in \mathcal{K}$ generates a sequence of length n using the process $\Pi_{X_k}^{\otimes n}$. The weight of these sequences is $\rho_k n \alpha_n$ on average. To be indistinguishable from the innocent distribution in the limit, the covert process $Q_{\alpha_n}^{\otimes n}$ has to satisfy

$$\lim_{n \to \infty} \mathbb{D}\big(Q_{\alpha_n}^{\otimes n} \| Q_{\emptyset}^{\otimes n}\big) = \lim_{n \to \infty} n \mathbb{D}(Q_{\alpha_n} \| Q_{\emptyset}) = 0. \tag{3.16}$$

Our assumptions in Section 3.3 ensure that $\chi(\boldsymbol{\rho})$ is non-zero. Consequently, from the results of Lemma 2 and (3.16), we conclude that if we choose the sequence $\{\alpha_n\}_{n\in\mathbb{N}^*}$ such that $\lim_{n\to\infty} n\alpha_n^2 = 0$, our covert process $Q_{\alpha_n}^{\otimes n}$ is indistinguishable from $Q_{\emptyset}^{\otimes n}$ in the limit. Consequently, we will construct a coding scheme that emulates the covert process $Q_{\alpha_n}^{\otimes n}$ instead of $Q_{\emptyset}^{\otimes n}$. The prime benefit of using $Q_{\alpha_n}^{\otimes n}$ instead of $Q_{\emptyset}^{\otimes n}$ is that $Q_{\alpha_n}^{\otimes n}$ allows us to convey covert information through the use of 1 symbols. In particular, it is possible to choose $\{\alpha_n\}_{n\in\mathbb{N}^*}$ such that $\lim_{n\to\infty} n\alpha_n = \infty$ so that the number of information bits grows with n.

The *square-root law* follows from the constraint $\lim_{n\to\infty} n\alpha_n^2 = 0$, which forces the scaling of $n\alpha_n$ to be arbitrarily close to but not exceed $\sqrt{n}$. If $\chi(\boldsymbol{\rho}) = 0$ for some $\boldsymbol{\rho}$, one would need to push the approximation of $\mathbb{D}\big(Q_{\alpha_n}^{\otimes n} \| Q_{\emptyset}^{\otimes n}\big)$ at least to the order α_n^3 in Lemma 2. In turn, we would only need to choose a sequence such that $\lim_{n\to\infty} n\alpha_n^3 = 0$, effectively allowing the increase of the scaling of $n\alpha_n$ to be arbitrarily close to but not exceed $n^{2/3}$ and beating the square root law. The assumption that $\chi(\boldsymbol{\rho}) > 0$ made in Section 3.3 therefore excludes the (rare) situations in which the square root law can be beaten.

3.5 Main result

We characterize the covert capacity region of a K-user binary-input MAC in Theorem 2, with the achievability proof in Section 3.5.2 and the converse proof in Section 3.5.3. The proofs adapt channel resolvability and converse techniques used in [27] for point-to-point channels to the MACs. The achievability proof is an extension of [27], and we provide details in the appendix; the converse proof presents more challenges and is fully detailed.

3.5.1 Covert capacity region of the K-user binary-input MAC

Theorem 2. *For $\boldsymbol{\rho} \triangleq \{\rho_k\}_{k\in\mathcal{K}} \in [0,1]^K$ such that $\sum_{k\in\mathcal{K}} \rho_k = 1$, define*

$$\chi(\boldsymbol{\rho}) \triangleq \sum_z \frac{\left(\sum_{k\in\mathcal{K}} \rho_k \left(Q_k(z) - Q_\emptyset(z)\right)\right)^2}{Q_\emptyset(z)}. \tag{3.17}$$

For the K-user binary-input MAC described in Section 3.3, the covert capacity region is

$$\bigcup_{\{\rho_k\}_{k\in\mathcal{K}}\in[0,1]^K:\sum_{k\in\mathcal{K}}\rho_k=1} \left\{ \{r_k\}_{k\in\mathcal{K}} : \forall k \in \mathcal{K}, \quad r_k \leqslant \sqrt{\frac{2}{\chi\left(\boldsymbol{\rho}\right)}} \rho_k \mathbb{D}(P_k \| P_\emptyset) \right\}. \tag{3.18}$$

In addition, for any achievable reliable and covert throughput tuple $r[\mathcal{K}]$ on the boundary of the covert capacity region characterized by $\boldsymbol{\rho}$, the set of achievable key throughput tuples is

$$\left\{ \{s_k\}_{k\in\mathcal{K}} : \forall k \in \mathcal{K}, \quad s_k \geqslant \sqrt{\frac{2}{\chi(\boldsymbol{\rho})}} \rho_k \left[\mathbb{D}(Q_k \| Q_\emptyset) - \mathbb{D}(P_k \| P_\emptyset)\right]^+ \right\}. \tag{3.19}$$

Note that $\chi\left(\boldsymbol{\rho}\right)$ in (3.17) is positive under the assumption made in Section 3.3, so that the bounds in (3.18) and (3.19) are well defined and finite. A few remarks are now in order.

- Our characterization of the covert capacity region only involves constraints on individual user's throughputs; there are no active constraints on the sum throughput. However, the individual throughputs are not identical to those of the single-user case [27], as there exists a non-trivial interplay among the ρ_k's, for $k \in \mathcal{K}$, through $\chi(\boldsymbol{\rho})$ in (3.18).

- User $k \in \mathcal{K}$ can achieve its maximum covert and reliable throughput without a

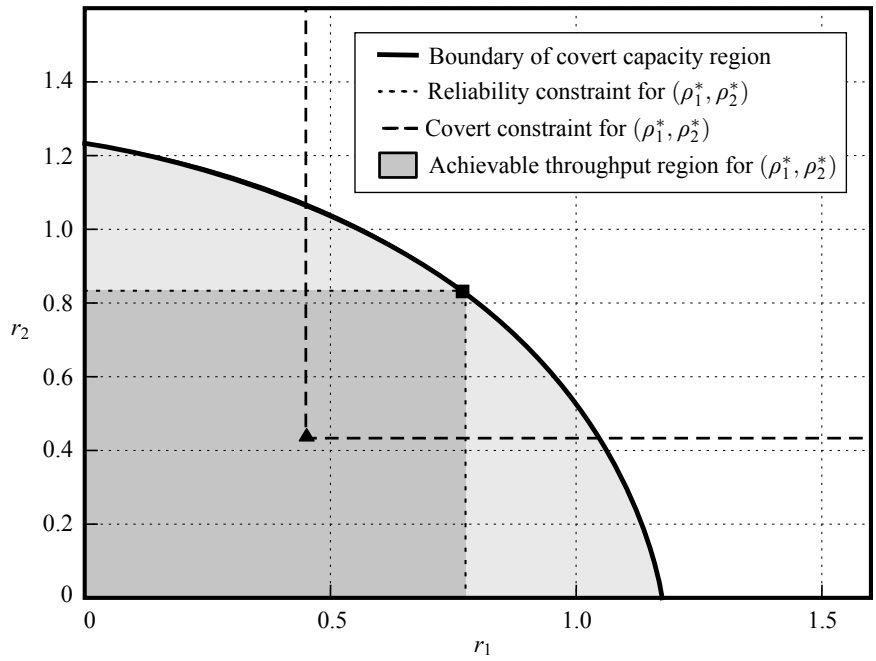

Figure 3.2: Representative example of the covert capacity region for a 2-user MAC. The achievable rate region for a specific choice of $\boldsymbol{\rho} = \boldsymbol{\rho}^* = (\rho_1^*, \rho_2^*)$ is highlighted.

key only if

$$\mathbb{D}(P_k \| P_\emptyset) \geqslant \mathbb{D}(Q_k \| Q_\emptyset), \tag{3.20}$$

is satisfied; that is, no secret key is required for user k if the channel from user k to the receiver is *better* than the channel to the warden when all other users are silent.

- If the MAC is symmetric, in the sense that $\forall z \in \mathcal{Z}$ and $\forall k \in \mathcal{K}$, $Q_k(z) = Q(z)$, then $\sum_{k \in \mathcal{K}} \rho_k \left(Q_k(z) - Q_\emptyset(z) \right) = Q(z) - Q_\emptyset(z)$, so that $\chi(\boldsymbol{\rho})$ is independent of $\boldsymbol{\rho}$ and time sharing is optimal.

Figure 3.2 illustrates the covert capacity region for a 2-user MAC with randomly generated channel matrices, $W_{Y|X_1X_2}$ and $W_{Z|X_1X_2}$, that satisfy (3.20) for $k \in \{1, 2\}$ and the absolute continuity requirements described in Section 3.3 for $\mathcal{K} = \{1, 2\}$. The thick solid curve denotes the boundary of the covert capacity region. All points on

this boundary can be achieved by varying the values of (ρ_1, ρ_2). For $\boldsymbol{\rho} = \boldsymbol{\rho}^* \triangleq (\rho_1^*, \rho_2^*)$, the achievable covert throughput region is highlighted in Figure 3.2, where the square marker represents the maximum achievable covert throughput pair $\left(\sqrt{\frac{2}{\chi(\boldsymbol{\rho}^*)}}\rho_1^*\mathbb{D}(P_1\|P_\emptyset), \sqrt{\frac{2}{\chi(\boldsymbol{\rho}^*)}}\rho_2^*\mathbb{D}(\right.$ while the triangular marker represents the pair $\left(\sqrt{\frac{2}{\chi(\boldsymbol{\rho}^*)}}\rho_1^*\mathbb{D}(Q_1\|Q_\emptyset), \sqrt{\frac{2}{\chi(\boldsymbol{\rho}^*)}}\rho_2^*\mathbb{D}(Q_2\|Q_\emptyset)\right)$. A non-empty intersection of the region to the top-right of the triangular marker and the region to the bottom-left of the square marker implies the existence of keyless covert communication schemes. If the regions do not intersect, a secret key is required to communicate covertly. Note that, for a symmetric 2-user MAC, the boundary of the covert capacity region is a straight line, and time sharing is optimal.

3.5.2 Achievability proof

We consider a communication scheme in which every user k employs L_k sub-codebooks, each consisting of M_k codewords. The value of the key $S_k \in [\![1, L_k]\!]$ chooses the sub-codebook that user k uses to encode its message $W_k \in [\![1, M_k]\!]$. The decoder, which possesses complete knowledge of the keys $S[\mathcal{K}]$, attempts to decode the messages sent by the K transmitters. The idea underlying the scheme is to use channel resolvability techniques to ensure that the total number of codewords is sufficiently large to keep the warden confused, while simultaneously ensuring that each sub-codebook is small enough for the receiver to reliably decode the messages.

Proposition 1. *Let* $\boldsymbol{\rho} \triangleq \{\rho_k\}_{k\in\mathcal{K}} \in [0,1]^K$ *with* $\sum_{k\in\mathcal{K}} \rho_k = 1$. *Let* $\{\alpha_n\}_{n\in\mathbb{N}^*}$ *be such that* $\alpha_n \in (0,1)$, $\lim_{n\to\infty} n\alpha_n = \infty$, *and* $\lim_{n\to\infty} n\alpha_n^2 = 0$. *For the channel model described in Section 3.3, for an arbitrary* $\mu \in (0,1)$, *there exist covert communication*

schemes such that $\forall k \in \mathcal{K}$,

$$r_k = (1-\mu)\sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k \mathbb{D}(P_k \| P_\emptyset), \tag{3.21}$$

$$s_k = \sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k \left[(1+\mu)\,\mathbb{D}(Q_k \| Q_\emptyset) - (1-\mu)\,\mathbb{D}(P_k \| P_\emptyset)\right]^+, \tag{3.22}$$

$$\lim_{n\to\infty} P_e^n = 0, \tag{3.23}$$

$$\lim_{n\to\infty} \mathbb{D}\Big(\widehat{Q}^n \| Q_\emptyset^{\otimes n}\Big) = 0. \tag{3.24}$$

Proof. To prove Proposition 1, we rely on random coding arguments for channel reliability and channel resolvability. However, the use of low-weight codewords in our communication scheme requires that we handle concentration inequalities carefully. Since basic concentration inequalities do not apply in the low-weight regime [27], we use Bernstein's inequality to establish our random coding arguments. The proof follows otherwise along the lines of [27, Theorem 2].

Random codebook generation At each transmitter $k \in \mathcal{K}$, generate $M_k L_k$ codewords $\mathbf{x}_k(m_k, \ell_k) \in \mathcal{X}^n$, where $(m_k, \ell_k) \in [\![1, M_k]\!] \times [\![1, L_k]\!]$, independently at random according to the distribution $\Pi_{X_k}^{\otimes n}$. For a set $\mathcal{T} \subset \mathcal{K}$, define

$$W_{Y|X[\mathcal{T}]}^{\otimes n}(\mathbf{y}|\mathbf{x}[\mathcal{T}]) \triangleq \sum_{\mathbf{x}[\mathcal{T}^c]} W_{Y|X[\mathcal{K}]}^{\otimes n}(\mathbf{y}|\mathbf{x}[\mathcal{K}]) \left(\prod_{k\in\mathcal{T}^c} \Pi_{X_k}^{\otimes n}(\mathbf{x}_k)\right). \tag{3.25}$$

Note that $W_{Y|X[\mathcal{T}]}^{\otimes n}$ is a product distribution since each user $k \in \mathcal{K}$ generates its codeword according to an n-fold product distribution $\Pi_{X_k}^{\otimes n}$. Also, note that if $\mathcal{T} = \emptyset$, $W_{Y|X[\mathcal{T}]}^{\otimes n} = P_{\alpha_n}^{\otimes n}$. Define the set $\mathcal{A}_\gamma^n \triangleq \bigcap_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \mathcal{A}_{\gamma_\mathcal{T}}^n$ with

$$\mathcal{A}_{\gamma_\mathcal{T}}^n \triangleq \left\{(\mathbf{x}[\mathcal{K}], \mathbf{y}) \in \mathcal{X}^n[\mathcal{K}] \times \mathcal{Y}^n : \log \frac{W_{Y|X[\mathcal{K}]}^{\otimes n}(\mathbf{y}|\mathbf{x}[\mathcal{K}])}{W_{Y|X[\mathcal{T}^c]}^{\otimes n}(\mathbf{y}|\mathbf{x}[\mathcal{T}^c])} \geqslant \gamma_\mathcal{T}\right\}, \tag{3.26}$$

where $\gamma_{\mathcal{T}} \triangleq (1-\mu)\, n\mathbb{I}(X[\mathcal{T}];Y|X[\mathcal{T}^c])$ for every non-empty set $\mathcal{T} \subseteq \mathcal{K}$ and an arbitrary $\mu \in (0,1)$. Encoder $k \in \mathcal{K}$ uses the key $S_k = \ell_k$ to map the message $W_k = m_k$ onto the codeword $\mathbf{x}_k(m_k, \ell_k)$. The codewords are then transmitted through the memoryless MAC to the legitimate receiver. The decoder, which observes $\mathbf{y}$ and has complete knowledge of the keys $\ell[\mathcal{K}]$, operates as follows.

- If there exists a unique $m[\mathcal{K}] \in \times_{k=1}^{K} [\![1, M_k]\!]$ such that $(\mathbf{x}_{\mathcal{K}}(m[\mathcal{K}], \ell[\mathcal{K}]), \mathbf{y}) \in \mathcal{A}_{\gamma}^{n}$, output $\widehat{W}[\mathcal{K}] = m[\mathcal{K}]$,
- Else, declare a decoding error.

Channel reliability analysis The decoding error probability P_e^n averaged over all random codebooks satisfies the following.

Lemma 3. *For any $\mu \in (0,1)$, an n large enough, and*

$$\log M_k = (1-\mu)\, \rho_k n \alpha_n \mathbb{D}(P_k \| P_\emptyset), \tag{3.27}$$

for every $k \in \mathcal{K}$, the probability of decoding error averaged over all random codebooks satisfies

$$\mathbb{E}(P_e^n) \leqslant \exp(-\xi n \alpha_n), \tag{3.28}$$

for an appropriate $\xi > 0$.

The proof of Lemma 3 is provided in Appendix 3.D.

Channel resolvability analysis In the following lemma, we show that the KL divergence between the induced distribution and the covert stochastic process averaged over all random codebooks vanishes in the limit.

Lemma 4. *For any $\mu \in (0,1)$, an n large enough, and*

$$\log M_k L_k = (1+\mu)\,\rho_k n \alpha_n \mathbb{D}(Q_k \| Q_\emptyset), \tag{3.29}$$

for every $k \in \mathcal{K}$, the KL divergence between $\widehat{Q}^n$ and $Q_{\alpha_n}^{\otimes n}$ averaged over all random codebooks satisfies

$$\mathbb{E}\left(\mathbb{D}\left(\widehat{Q}^n \| Q_{\alpha_n}^{\otimes n}\right)\right) \leqslant \exp\left(-\xi n \alpha_n\right), \tag{3.30}$$

for an appropriate $\xi > 0$.

The proof of Lemma 4 is provided in Appendix 3.E.

Identification of a specific code Using Markov's inequality, we obtain

$$\mathbb{P}\left(P_e^n < 4\mathbb{E}\left(P_e^n\right) \cap \mathbb{D}\left(\widehat{Q}^n \| Q_{\alpha_n}^{\otimes n}\right) < 4\mathbb{E}\left(\mathbb{D}\left(\widehat{Q}^n \| Q_{\alpha_n}^{\otimes n}\right)\right)\right) \geqslant \frac{1}{2}. \tag{3.31}$$

Then, we conclude that there must exist at least one coding scheme such that for appropriate constants $\xi_1, \xi_2 > 0$ and an n large enough, we have

$$P_e^n \leqslant \exp\left(-\xi_1 n \alpha_n\right), \tag{3.32}$$

$$\mathbb{D}\left(\widehat{Q}^n \| Q_{\alpha_n}^{\otimes n}\right) \leqslant \exp\left(-\xi_2 n \alpha_n\right). \tag{3.33}$$

Lemma 5. *For n large enough and an appropriate constant $\xi_3 > 0$,*

$$\left|\mathbb{D}\left(\widehat{Q}^n \| Q_\emptyset^{\otimes n}\right) - \mathbb{D}\left(Q_{\alpha_n}^{\otimes n} \| Q_\emptyset^{\otimes n}\right)\right| \leqslant \exp\left(-\xi_3 n \alpha_n\right), \tag{3.34}$$

provided $\mathbb{D}\left(\widehat{Q}^n \| Q_{\alpha_n}^{\otimes n}\right)$ satisfies (3.33).

The proof of Lemma 5 is provided in Appendix 3.F. Using (3.14), (3.32), (3.34), and our choice of $\{\alpha_n\}_{n \in \mathbb{N}^*}$, we conclude that there exists at least one coding scheme

that satisfies (3.23) and (3.24). Combining (3.14) and (3.34) yields

$$\frac{n\alpha_n^2}{2}\left(1+\sqrt{\alpha_n}\right)\chi_n(\boldsymbol{\rho})+\exp\left(-\xi_3 n\alpha_n\right)\geqslant \mathbb{D}\Big(\widehat{Q}^n\|Q_\emptyset^{\otimes n}\Big) \\ \geqslant \frac{n\alpha_n^2}{2}\left(1-\sqrt{\alpha_n}\right)\chi_n(\boldsymbol{\rho})-\exp\left(-\xi_3 n\alpha_n\right). \tag{3.35}$$

We normalize $\log M_k$, where $k\in\mathcal{K}$, by $\sqrt{n\mathbb{D}\Big(\widehat{Q}^n\|Q_\emptyset^{\otimes n}\Big)}$ using (3.27), (3.29), and (3.35) to obtain

$$\lim_{n\to\infty}\frac{\log M_k}{\sqrt{n\mathbb{D}\Big(\widehat{Q}^n\|Q_\emptyset^{\otimes n}\Big)}}=(1-\mu)\sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k\mathbb{D}(P_k\|P_\emptyset), \tag{3.36}$$

$$\lim_{n\to\infty}\frac{\log M_k L_k}{\sqrt{n\mathbb{D}\Big(\widehat{Q}^n\|Q_\emptyset^{\otimes n}\Big)}}=(1+\mu)\sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k\mathbb{D}(Q_k\|Q_\emptyset). \tag{3.37}$$

Combining (3.36) and (3.37), we obtain

$$\lim_{n\to\infty}\frac{\log L_k}{\sqrt{n\mathbb{D}\Big(\widehat{Q}^n\|Q_\emptyset^{\otimes n}\Big)}}=\sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k\left[(1+\mu)\,\mathbb{D}(Q_k\|Q_\emptyset)-(1-\mu)\,\mathbb{D}(P_k\|P_\emptyset)\right]^+. \tag{3.38}$$

□

Since μ in (3.21) is arbitrary, we conclude from Proposition 1 that the covert capacity region contains the region defined by

$$\bigcup_{\{\rho_k\}_{k\in\mathcal{K}}\in[0,1]^K:\sum_{k\in\mathcal{K}}\rho_k=1}\left\{\{r_k\}_{k\in\mathcal{K}}:\forall k\in\mathcal{K},\quad r_k\leqslant\sqrt{\frac{2}{\chi\left(\boldsymbol{\rho}\right)}}\rho_k\mathbb{D}(P_k\|P_\emptyset)\right\}. \tag{3.39}$$

In addition, any achievable covert throughput tuple $r\left[\mathcal{K}\right]$ that is characterized by a specific $\boldsymbol{\rho}$ and lies on the boundary of the region defined in (3.39) is associated with an achievable key throughput tuple $\left\{\sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k\left[\mathbb{D}(Q_k\|Q_\emptyset)-\mathbb{D}(P_k\|P_\emptyset)\right]^+\right\}_{k\in\mathcal{K}}$.

3.5.3 Converse proof

Proposition 2. *For the channel model described in Section 3.3, consider a sequence of covert communication schemes with increasing blocklength $n \in \mathbb{N}^*$ characterized by $\epsilon_n \triangleq P_e^n$ and $\delta_n \triangleq \mathbb{D}\Big(\widehat{Q}^n \| Q_\emptyset^{\otimes n}\Big)$ such that $\lim_{n\to\infty} \epsilon_n = 0$ and $\lim_{n\to\infty} \delta_n = 0$. Then, there exists a vector $\boldsymbol{\rho} \triangleq \{\rho_k\}_{k\in\mathcal{K}} \in [0,1]^K$ with $\sum_{k\in\mathcal{K}} \rho_k = 1$ and an infinite subset $\mathcal{N} \subseteq \mathbb{N}^*$, such that for all $k \in \mathcal{K}$,*

$$\liminf_{\substack{n\to\infty \\ n\in\mathcal{N}}} \frac{\log M_k}{\sqrt{n\delta_n}} \leqslant \sqrt{\frac{2}{\chi(\boldsymbol{\rho})}} \rho_k \mathbb{D}(P_k \| P_\emptyset). \tag{3.40}$$

For a sequence of codes that achieves the right hand side of (3.40) *for all $k \in \mathcal{K}$, we have*

$$\limsup_{\substack{n\to\infty \\ n\in\mathcal{N}}} \frac{\log M_k L_k}{\sqrt{n\delta_n}} \geqslant \sqrt{\frac{2}{\chi(\boldsymbol{\rho})}} \rho_k \mathbb{D}(Q_k \| Q_\emptyset), \tag{3.41}$$

for all $k \in \mathcal{K}$.

Proof. Consider a sequence of covert communication schemes with increasing blocklength n characterized by $\epsilon_n \triangleq P_e^n$ and $\delta_n \triangleq \mathbb{D}\Big(\widehat{Q}^n \| Q_\emptyset^{\otimes n}\Big)$, and $\log M_k$ takes the maximum value such that $\lim_{n\to\infty} \log M_k = \infty$ for all $k \in \mathcal{K}$. Each user k transmits an $n-$length codeword $\mathbf{X}_k = (X_{k1}, X_{k2}, \ldots, X_{kn}) \in \mathcal{X}^n$, where $n \in \mathbb{N}^*$, to the receiver. For $j \in [\![1, n]\!]$, we denote the distribution of each symbol X_{kj} on $\mathcal{X}$ by $\Pi_{X_{kj}}$, where

$$\Pi_{X_{kj}}(x) \triangleq \frac{\sum_{m_k=1}^{M_k} \sum_{\ell_k=1}^{L_k} \mathbb{1}\{X_{kj}(m_k, \ell_k) = x\}}{M_k L_k}. \tag{3.42}$$

We define $\Pi_{X_{kj}}(1) = 1 - \Pi_{X_{kj}}(0) \triangleq \mu_{kj}^{(n)}$. Note that $\mu_{kj}^{(n)}$ depends on n, the transmitter index k, and the symbol position j. For every $n \in \mathbb{N}^*$, we define a permutation $\pi_{k^*}^{(n)}$

of $[\![1,n]\!]$ to define a new code such that

$$(k^*,1) = \arg \max_{(k,j)\in\mathcal{K}\times[\![1,n]\!]} \mu_{kj}^{(n)}. \tag{3.43}$$

Since the channel is memoryless, the performance of the new code that satisfies (3.43) matches that of the original code. Hence, without loss of generality, we only study the sequence of codes for which (3.43) holds for every $n \in \mathbb{N}^*$. Note that the sequence $\left\{\{\mu_{k1}^{(n)}\}_{k\in\mathcal{K}}\right\}_{n\in\mathbb{N}^*}$ belongs to $[0,1]^K$ which is a closed and bounded set. Hence, we can extract a convergent subsequence $\left\{\{\mu_{k1}^{(n)}\}_{k\in\mathcal{K}}\right\}_{n\in\mathcal{N}^*}$, where $\mathcal{N}^* \subseteq \mathbb{N}^*$ is an infinite set, with limit $\{\mu_{k1}^*\}_{k\in\mathcal{K}}$. Let us now assume that the sequence $\{\mu_{k1}^*\}_{k\in\mathcal{K}} \in [0,1]^K$ is not an all-zero sequence.

For $j \in [\![1,n]\!]$, we denote the K-length vector $\{x_{kj}\}_{k\in\mathcal{K}}$ by $x_{(j)}[\mathcal{K}]$. The warden makes an observation $\mathbf{Z}$ of length n, whose distribution is denoted by $\widehat{Q}^n$. For $j \in [\![1,n]\!]$, we denote the distribution of each component Z_j of $\mathbf{Z}$ by $\widehat{Q}_j$, where

$$\widehat{Q}_j(z) \triangleq \frac{1}{\prod_{k\in\mathcal{K}} M_k L_k} \sum_{m[\mathcal{K}]} \sum_{\ell[\mathcal{K}]} W_{Z|X[\mathcal{K}]}(z|\{x_{kj}(m_k,\ell_k)\}_{k\in\mathcal{K}}) \tag{3.44}$$

$$= \sum_{x_{(j)}[\mathcal{K}]} \left(\prod_{k\in\mathcal{K}} \Pi_{X_{kj}}(x_{kj})\right) W_{Z|X[\mathcal{K}]}\left(z|x_{(j)}[\mathcal{K}]\right) \tag{3.45}$$

$$\overset{(a)}{=} \sum_{\mathcal{T}\subseteq\mathcal{K}} \left(\prod_{k\in\mathcal{T}} \mu_{kj}^{(n)}\right)\left(\prod_{k\in\mathcal{T}^c}\left(1-\mu_{kj}^{(n)}\right)\right) Q_{\mathcal{T}}(z), \tag{3.46}$$

where (a) follows from the definition of $Q_{\mathcal{T}}(z) \triangleq W_{Z|X[\mathcal{K}]}(z|x_{\mathcal{T}})$ in (3.1). Alternatively, using Lemma 6 in the appendix, we write

$$\widehat{Q}_j(z) = Q_{\emptyset}(z) + \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \left(\prod_{k\in\mathcal{T}} \mu_{kj}^{(n)}\right) G_{\mathcal{T}}(z). \tag{3.47}$$

From the definition of δ_n, we have

$$\delta_n = \mathbb{D}\Big(\widehat{Q}^n \| Q_\emptyset^{\otimes n}\Big) \tag{3.48}$$

$$= -\mathbb{H}(\mathbf{Z}) + \mathbb{E}\left([]\,\widehat{Q}^n\right] \log \frac{1}{Q_\emptyset^{\otimes n}(\mathbf{Z})} \tag{3.49}$$

$$= -\left(\sum_{j=1}^{n} \mathbb{H}\big(Z_j|\mathbf{Z}^{j-1}\big)\right) + \mathbb{E}\left([]\,\widehat{Q}^n\right] \sum_{j=1}^{n} \log \frac{1}{Q_\emptyset(Z_j)} \tag{3.50}$$

$$\overset{(a)}{\geqslant} \sum_{j=1}^{n} \left(-\mathbb{H}(Z_j) + \mathbb{E}\left([]\,\widehat{Q}_j\right] \log \frac{1}{Q_\emptyset(Z_j)}\right) \tag{3.51}$$

$$= \sum_{j=1}^{n} \mathbb{D}\Big(\widehat{Q}_j \| Q_\emptyset\Big), \tag{3.52}$$

where (a) follows from the fact that conditioning reduces entropy. Since $\lim_{n\to\infty} \delta_n = 0$ and KL divergence is non-negative, it follows from (3.52) that

$$\lim_{n\to\infty} \mathbb{D}\Big(\widehat{Q}_j \| Q_\emptyset\Big) = 0, \tag{3.53}$$

for all $j \in [\![1, n]\!]$. Applying Pinsker's inequality on (3.53), we obtain $\lim_{n\to\infty} \mathbb{V}\Big(\widehat{Q}_j, Q_\emptyset\Big) = 0$, which implies that $\forall z \in \mathcal{Z}$,

$$\lim_{n\to\infty} \left|\widehat{Q}_j(z) - Q_\emptyset(z)\right| = 0, \tag{3.54}$$

$$\lim_{n\to\infty} \widehat{Q}_j(z) = Q_\emptyset(z). \tag{3.55}$$

Fixing $j = 1$ and by using (3.46) and (3.55), for $n \in \mathcal{N}^*$, we obtain

$$\lim_{\substack{n\to\infty \\ n\in\mathcal{N}^*}} \left(\sum_{\mathcal{T}\subseteq\mathcal{K}} \left(\prod_{k\in\mathcal{T}} \mu_{k1}^{(n)}\right) \left(\prod_{k\in\mathcal{T}^c} \left(1 - \mu_{k1}^{(n)}\right)\right) Q_\mathcal{T}(z)\right) = Q_\emptyset(z), \tag{3.56}$$

$$\sum_{\mathcal{T}\subseteq\mathcal{K}} \left(\prod_{k\in\mathcal{T}} \mu_{k1}^{*}\right) \left(\prod_{k\in\mathcal{T}^c} \left(1 - \mu_{k1}^{*}\right)\right) Q_\mathcal{T}(z) = Q_\emptyset(z). \tag{3.57}$$

Since we assumed that the sequence $\{\mu_{k1}^*\}_{k\in\mathcal{K}}$ is not an all-zero sequence, (3.57)

implies that $Q_\emptyset$ is a convex combination of $\{Q_\mathcal{T}\}_{\mathcal{T}\subseteq\mathcal{K}:\,\mathcal{T}\neq\emptyset}$. Note that the convex combination in (3.57) does not require the transmitters to coordinate, which is the case in our channel model, since the input from each user is independent of the inputs from other users. Since (3.57) contradicts the assumption made in Section 3.3, our assumption about $\{\mu_{k1}^*\}_{k\in\mathcal{K}}$ is incorrect, and we have

$$\lim_{\substack{n\to\infty\\ n\in\mathcal{N}^*}} \mu_{k1}^{(n)} = 0, \tag{3.58}$$

for all $k \in \mathcal{K}$, which implies that

$$\lim_{\substack{n\to\infty\\ n\in\mathcal{N}^*}} \mu_{k^*1}^{(n)} = 0. \tag{3.59}$$

Subsequently, from (3.43) and (3.59), we obtain

$$\lim_{\substack{n\to\infty\\ n\in\mathcal{N}^*}} \mu_{kj}^{(n)} = 0, \tag{3.60}$$

for all $(k, j) \in \mathcal{K} \times [\![1, n]\!]$. Henceforth, we only consider the subsequence of codes with blocklength $n \in \mathcal{N}^*$. Next, for $j \in [\![1, n]\!]$, define

$$\Psi_j^{(n)}(z) \triangleq \widehat{Q}_j(z) - Q_\emptyset(z). \tag{3.61}$$

Note that $\sum_z \Psi_j^{(n)}(z) = 0$. Also note that from (3.54) and (3.61), we have $\lim_{n\to\infty} \Psi_j^{(n)}(z) = 0$ for all $j \in [\![1, n]\!]$ and $\forall z \in \mathcal{Z}$. We lower bound $\mathbb{D}\Big(\widehat{Q}_j \| Q_\emptyset\Big)$ for n large enough by

$$\mathbb{D}\Big(\widehat{Q}_j \| Q_\emptyset\Big) = \sum_z \widehat{Q}_j(z) \log \frac{\widehat{Q}_j(z)}{Q_\emptyset(z)} \tag{3.62}$$

$$= \sum_z Q_\emptyset(z) \left(1 + \frac{\Psi_j^{(n)}(z)}{Q_\emptyset(z)}\right) \log \left(1 + \frac{\Psi_j^{(n)}(z)}{Q_\emptyset(z)}\right) \tag{3.63}$$

$$\overset{(a)}{\geqslant} \sum_z \left(\frac{\left(\Psi_j^{(n)}(z)\right)^2}{2Q_\emptyset(z)} - \frac{\left(\Psi_j^{(n)}(z)\right)^3}{2Q_\emptyset^2(z)} \right) + \sum_{z:\Psi_j^{(n)}(z)<0} \frac{2\left(\Psi_j^{(n)}(z)\right)^3}{3Q_\emptyset^2(z)} \tag{3.64}$$

$$\geqslant \sum_z \frac{\left(\Psi_j^{(n)}(z)\right)^2}{2Q_\emptyset(z)} \left(1 - \frac{\Psi_j^{(n)}(z)}{Q_\emptyset(z)} - \frac{4\left|\Psi_j^{(n)}(z)\right|}{3Q_\emptyset(z)} \right), \tag{3.65}$$

where (a) follows from the inequality $\log(1+x) > x - \frac{x^2}{2}$ for $x \geqslant 0$ and[4] $\log(1+x) > x - \frac{x^2}{2} + \frac{2x^3}{3}$ for $x \in \left[-\frac{1}{2}, 0\right]$. For $j \in [\![1,n]\!]$, define $\xi_j^{(n)}(z) \triangleq \frac{\Psi_j^{(n)}(z)}{Q_\emptyset(z)} + \frac{4\left|\Psi_j^{(n)}(z)\right|}{3Q_\emptyset(z)}$ and $\xi^{(n)}(z) \triangleq \max_{j\in[\![1,n]\!]} \xi_j^{(n)}(z)$. Since $\lim_{n\to\infty} \Psi_j^{(n)}(z) = 0$, we have $\lim_{n\to\infty} \xi_j^{(n)}(z) = 0$ for all $j \in [\![1,n]\!]$. From (3.47) and (3.61), for $j \in [\![1,n]\!]$, we write

$$\left|\Psi_j^{(n)}(z)\right| = \left|\widehat{Q}_j(z) - Q_\emptyset(z)\right| \tag{3.66}$$

$$\leqslant \sum_{\mathcal{T}\subseteq\mathcal{K}:\mathcal{T}\neq\emptyset} \left(\prod_{k\in\mathcal{T}} \mu_{kj}^{(n)} \right) |G_\mathcal{T}(z)| \tag{3.67}$$

$$\overset{(a)}{\leqslant} \mu_{k^*1}^{(n)} \left(\sum_{\mathcal{T}\subseteq\mathcal{K}:\mathcal{T}\neq\emptyset} |G_\mathcal{T}(z)| \right), \tag{3.68}$$

where (a) follows from (3.43) and the fact that $\mu_{kj}^{(n)} \in [0,1]$ for all $k \in \mathcal{K}$ and $j \in [\![1,n]\!]$. Note that the term inside the parentheses in (3.68) is positive and bounded. Consequently, for $z \in \mathcal{Z}$,

$$\max_{j\in[\![1,n]\!]} \left|\Psi_j^{(n)}(z)\right| \leqslant \mu_{k^*1}^{(n)} \left(\sum_{\mathcal{T}\subseteq\mathcal{K}:\mathcal{T}\neq\emptyset} |G_\mathcal{T}(z)| \right). \tag{3.69}$$

From the definition of $\xi_j^{(n)}(z)$, we have

$$\xi_j^{(n)}(z) = \frac{\Psi_j^{(n)}(z)}{Q_\emptyset(z)} + \frac{4\left|\Psi_j^{(n)}(z)\right|}{3Q_\emptyset(z)} \tag{3.70}$$

[4]Note that for n large enough, we can ensure that $\Psi_j^{(n)}(z) \in \left[-\frac{1}{2}, 0\right]$ if $\Psi_j^{(n)}(z) < 0$ since $\lim_{n\to\infty} \Psi_j^{(n)}(z) = 0$.

$$\leqslant \frac{\left|\Psi_j^{(n)}(z)\right|}{Q_\emptyset(z)} + \frac{4\left|\Psi_j^{(n)}(z)\right|}{3Q_\emptyset(z)} \tag{3.71}$$

$$= \frac{7\left|\Psi_j^{(n)}(z)\right|}{3Q_\emptyset(z)}. \tag{3.72}$$

Consequently, we have

$$\xi^{(n)}(z) = \max_{j\in[\![1,n]\!]} \xi_j^{(n)}(z) \tag{3.73}$$

$$\leqslant \frac{7}{3Q_\emptyset(z)} \max_{j\in[\![1,n]\!]} \left|\Psi_j^{(n)}(z)\right| \tag{3.74}$$

$$\leqslant \frac{7}{3Q_\emptyset(z)} \mu_{k^*1}^{(n)} \left(\sum_{\mathcal{T}\subseteq\mathcal{K}:\mathcal{T}\neq\emptyset} |G_{\mathcal{T}}(z)| \right). \tag{3.75}$$

Note that, by definition, $\xi_j^{(n)}(z)$ is non-negative irrespective of the sign of $\Psi_j^{(n)}(z)$. Then, using (3.59) and (3.75), we conclude that $\lim_{\substack{n\to\infty \\ n\in\mathcal{N}^*}} \xi^{(n)}(z) = 0$. Using (3.65), we lower bound (3.52) by

$$\delta_n \geqslant \sum_{j=1}^{n} \sum_{z} \frac{\left(\Psi_j^{(n)}(z)\right)^2}{2Q_\emptyset(z)} \left(1 - \xi_j^{(n)}(z)\right) \tag{3.76}$$

$$\geqslant \sum_{z} \frac{\left(1-\xi^{(n)}(z)\right)}{2Q_\emptyset(z)} \sum_{j=1}^{n} \left(\Psi_j^{(n)}(z)\right)^2. \tag{3.77}$$

For $k \in \mathcal{K}$, we upper bound $\log M_k$ using standard techniques,

$$\log M_k \overset{(a)}{\leqslant} \mathbb{I}(W_k; \mathbf{Y}S_k) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M_k \tag{3.78}$$

$$\leqslant \mathbb{I}(W_k S_k; \mathbf{Y}) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M_k \tag{3.79}$$

$$= \mathbb{I}(\mathbf{X}_k; \mathbf{Y}) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M_k \tag{3.80}$$

$$= \mathbb{H}(\mathbf{X}_k) - \mathbb{H}(\mathbf{X}_k|\mathbf{Y}) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M_k \tag{3.81}$$

$$\overset{(b)}{\leqslant} \mathbb{H}(\mathbf{X}_k|\mathbf{X}\left[\mathcal{K}\setminus\{k\}\right]) - \mathbb{H}(\mathbf{X}_k|\mathbf{Y}\mathbf{X}\left[\mathcal{K}\setminus\{k\}\right]) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M_k \tag{3.82}$$

$$= \mathbb{I}(\mathbf{X}_k; \mathbf{Y}|\mathbf{X}\left[\mathcal{K}\setminus\{k\}\right]) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M_k \tag{3.83}$$

$$= \mathbb{H}(\mathbf{Y}|\mathbf{X}\left[\mathcal{K}\setminus\{k\}\right]) - \mathbb{H}(\mathbf{Y}|\mathbf{X}[\mathcal{K}]) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M_k \tag{3.84}$$

$$\overset{(c)}{\leqslant} \sum_{j=1}^{n} \mathbb{H}\big(Y_j|X_{(j)}\left[\mathcal{K}\setminus\{k\}\right]\big) - \sum_{j=1}^{n} \mathbb{H}\big(Y_j|X_{(j)}[\mathcal{K}]\big) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M_k \tag{3.85}$$

$$= \sum_{j=1}^{n} \mathbb{I}\big(X_{kj}; Y_j|X_{(j)}\left[\mathcal{K}\setminus\{k\}\right]\big) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M_k, \tag{3.86}$$

where (a) follows from Fano's inequality, (b) follows from the fact that $\mathbf{X}_k$ and $\mathbf{X}[\mathcal{K}\setminus\{k\}]$ are mutually independent and the fact that conditioning reduces entropy, and (c) follows from the fact that conditioning reduces entropy and the memoryless property of the channel. We expand the mutual information term in (3.86) as

$$\begin{aligned}
&\mathbb{I}\big(X_{kj}; Y_j|X_{(j)}\left[\mathcal{K}\setminus\{k\}\right]\big) \\
&= \sum_{\mathcal{T}\subseteq\mathcal{K}} \left(\prod_{i\in\mathcal{K}} \Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right) \mathbb{D}\Big(P_{\mathcal{T}}\|W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]=x_{\mathcal{T}}[\mathcal{K}\setminus\{k\}]}\Big) &(3.87)\\
&= \sum_{\mathcal{T}\subseteq\mathcal{K}} \left(\prod_{i\in\mathcal{K}} \Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right) \mathbb{D}(P_{\mathcal{T}}\|P_{\emptyset}) \\
&\quad - \sum_{y}\sum_{\mathcal{T}\subseteq\mathcal{K}} \left(\prod_{i\in\mathcal{K}} \Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right) P_{\mathcal{T}}\left(y\right) \log \frac{W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]}\left(y|x_{\mathcal{T}}\left[\mathcal{K}\setminus\{k\}\right]\right)}{P_{\emptyset}(y)}. &(3.88)
\end{aligned}$$

Defining $\mu_{\max}^{(n)} \triangleq \mu_{k^*1}^{(n)}$ and $d_1 \triangleq 2^K \max_{\mathcal{T}\subseteq\mathcal{K}:|\mathcal{T}|>1} \mathbb{D}(P_{\mathcal{T}}\|P_{\emptyset})$, we upper bound the first term in (3.88) by

$$\begin{aligned}
\sum_{\mathcal{T}\subseteq\mathcal{K}} \left(\prod_{i\in\mathcal{K}} \Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right) \mathbb{D}(P_{\mathcal{T}}\|P_{\emptyset}) &\overset{(a)}{=} \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ |\mathcal{T}|>1}} \left(\prod_{i\in\mathcal{T}} \mu_{ij}^{(n)}\right) \left(\prod_{i\in\mathcal{T}^c} \left(1-\mu_{ij}^{(n)}\right)\right) \mathbb{D}(P_{\mathcal{T}}\|P_{\emptyset}) \\
&\quad + \sum_{i\in\mathcal{K}} \mu_{ij}^{(n)} \left(\prod_{i'\in\mathcal{K}\setminus\{i\}} \left(1-\mu_{i'j}^{(n)}\right)\right) \mathbb{D}(P_i\|P_{\emptyset}) &(3.89)\\
&\overset{(b)}{\leqslant} d_1 \mu_{\max}^{(n)} \sum_{i\in\mathcal{K}} \mu_{ij}^{(n)} + \sum_{i\in\mathcal{K}} \mu_{ij}^{(n)} \mathbb{D}(P_i\|P_{\emptyset}), &(3.90)
\end{aligned}$$

where (a) follows from splitting the sum into two based on the number of $1'$s in $x_{\mathcal{T}}$, and (b) follows from the fact that $\left(1-\mu_{i'j}^{(n)}\right) \leqslant 1$ for all $(i', j) \in \mathcal{K} \times [\![1, n]\!]$. Defining $d_2 \triangleq 2^K \max_{i \in \mathcal{K}\setminus\{k\}} \mathbb{D}\Big(W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]=x_i[\mathcal{K}\setminus\{k\}]} \| P_\emptyset\Big)$, we lower bound the second term in (3.88) by

$$\sum_y \sum_{\mathcal{T}\subseteq\mathcal{K}} \left(\prod_{i\in\mathcal{K}} \Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right) P_{\mathcal{T}}\left(y\right) \log \frac{W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]}\left(y|x_{\mathcal{T}}\left[\mathcal{K}\setminus\{k\}\right]\right)}{P_\emptyset(y)}$$

$$= \sum_{\mathcal{T}\subseteq\mathcal{K}\setminus\{k\}} \left(\prod_{i\in\mathcal{K}\setminus\{k\}} \Pi_{X_{ij}}(x_{\mathcal{T},i})\right) \sum_y \sum_x \Pi_{X_{kj}}(x) W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]X_{kj}}\left(y|x_{\mathcal{T}}\left[\mathcal{K}\setminus\{k\}\right]x\right)$$
$$\times \log \frac{W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]}\left(y|x_{\mathcal{T}}[\mathcal{K}\setminus\{k\}]\right)}{P_\emptyset(y)} \tag{3.91}$$

$$\overset{(a)}{=} \sum_{\mathcal{T}\subseteq\mathcal{K}\setminus\{k\}} \left(\prod_{i\in\mathcal{K}\setminus\{k\}} \Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right) \mathbb{D}\Big(W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]=x_{\mathcal{T}}[\mathcal{K}\setminus\{k\}]} \| P_\emptyset\Big) \tag{3.92}$$

$$\geqslant \sum_{\mathcal{T}\subseteq\mathcal{K}\setminus\{k\}:|\mathcal{T}|=1} \left(\prod_{i\in\mathcal{K}\setminus\{k\}} \Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right) \mathbb{D}\Big(W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]=x_{\mathcal{T}}[\mathcal{K}\setminus\{k\}]} \| P_\emptyset\Big) \tag{3.93}$$

$$= \sum_{i\in\mathcal{K}\setminus\{k\}} \mu_{ij}^{(n)} \left(\prod_{i'\in\mathcal{K}\setminus\{i,k\}} \left(1-\mu_{i'j}^{(n)}\right)\right) \mathbb{D}\Big(W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]=x_i[\mathcal{K}\setminus\{k\}]} \| P_\emptyset\Big) \tag{3.94}$$

$$\overset{(b)}{=} \sum_{i\in\mathcal{K}\setminus\{k\}} \mu_{ij}^{(n)} \left(1 + \sum_{\mathcal{T}\subseteq\mathcal{K}\setminus\{i,k\}} (-1)^{|\mathcal{T}|} \left(\prod_{i'\in\mathcal{T}} \mu_{i'j}^{(n)}\right)\right) \mathbb{D}\Big(W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]=x_i[\mathcal{K}\setminus\{k\}]} \| P_\emptyset\Big) \tag{3.95}$$

$$\geqslant \sum_{i\in\mathcal{K}\setminus\{k\}} \mu_{ij}^{(n)} \left(1 - \sum_{\mathcal{T}\subseteq\mathcal{K}\setminus\{i,k\}:\ |\mathcal{T}| \text{ is odd}} \left(\prod_{i'\in\mathcal{T}} \mu_{i'j}^{(n)}\right)\right) \mathbb{D}\Big(W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]=x_i[\mathcal{K}\setminus\{k\}]} \| P_\emptyset\Big) \tag{3.96}$$

$$\geqslant \sum_{i\in\mathcal{K}\setminus\{k\}} \mu_{ij}^{(n)} \left(1 - 2^K \mu_{\max}^{(n)}\right) \mathbb{D}\Big(W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]=x_i[\mathcal{K}\setminus\{k\}]} \| P_\emptyset\Big) \tag{3.97}$$

$$\geqslant \sum_{i\in\mathcal{K}\setminus\{k\}} \mu_{ij}^{(n)} \mathbb{D}\Big(W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]=x_i[\mathcal{K}\setminus\{k\}]} \| P_\emptyset\Big) - d_2 \mu_{\max}^{(n)} \sum_{i\in\mathcal{K}\setminus\{k\}} \mu_{ij}^{(n)}, \tag{3.98}$$

where (a) follows from the fact that

$$\sum_{x} \Pi_{X_{kj}}(x) W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]X_{kj}}\left(y|x_{\mathcal{T}}\left[\mathcal{K}\setminus\{k\}\right]x\right) = W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]}\left(y|x_{\mathcal{T}}\left[\mathcal{K}\setminus\{k\}\right]\right), \tag{3.99}$$

and (b) follows from the fact that

$$\prod_{i'\in\mathcal{K}\setminus\{i,k\}} (1-\mu_{i'j}^{(n)}) = 1 + \sum_{\mathcal{T}\subseteq\mathcal{K}\setminus\{i,k\}} (-1)^{|\mathcal{T}|} \left(\prod_{i'\in\mathcal{T}} \mu_{i'j}^{(n)}\right). \tag{3.100}$$

Note that we can write $W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]}(y|x_i[\mathcal{K}\setminus\{k\}]) = (1-\mu_{kj}^{(n)})\, P_i(y) + \mu_{kj}^{(n)} P_{\{i,k\}}(y)$. We define $d_3 \triangleq \left|\sum_y \left(P_{\{i,k\}}(y) - P_i(y)\right) \log \frac{P_i(y)}{P_\emptyset(y)}\right|$. Note that d_3 is bounded since $P_i \ll P_\emptyset$. Then, we lower bound the KL divergence term in (3.98) by

$$\begin{aligned}
\mathbb{D}\Big(W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]=x_i[\mathcal{K}\setminus\{k\}]} \| P_\emptyset\Big) &= \sum_y W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]}\left(y|x_i\left[\mathcal{K}\setminus\{k\}\right]\right) \log \frac{P_i(y)}{P_\emptyset(y)} \\
&\quad + \mathbb{D}\Big(W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]=x_i[\mathcal{K}\setminus\{k\}]} \| P_i\Big) \qquad (3.101) \\
&\geqslant \sum_y P_i(y) \left(1 + \mu_{kj}^{(n)} \frac{P_{\{i,k\}}(y) - P_i(y)}{P_i(y)}\right) \log \frac{P_i(y)}{P_\emptyset(y)} \qquad (3.102) \\
&\geqslant \mathbb{D}(P_i\|P_\emptyset) - d_3 \mu_{\max}^{(n)}. \qquad (3.103)
\end{aligned}$$

Defining $d_4 \triangleq d_1 + d_2 + d_3$ and combining (3.88), (3.90), (3.98), and (3.103), we obtain

$$\mathbb{I}(X_{kj}; Y_j|X_j\left[\mathcal{K}\setminus\{k\}\right]) \leqslant \mu_{kj}^{(n)} \mathbb{D}(P_k\|P_\emptyset) + d_4 \mu_{\max}^{(n)} \sum_{i\in\mathcal{K}} \mu_{ij}^{(n)}. \tag{3.104}$$

Next, we normalize $\log M_k$, where $k \in \mathcal{K}$, by $\sqrt{n\delta_n}$. Using (3.77), (3.86), and (3.104),

for n large enough, we obtain

$$\frac{\log M_k}{\sqrt{n\delta_n}} \leqslant \frac{\sum_{j=1}^n \mu_{kj}^{(n)} \mathbb{D}(P_k \| P_\emptyset) + d_4 \mu_{\max}^{(n)} \sum_{i\in\mathcal{K}} \sum_{j=1}^n \mu_{ij}^{(n)} + \mathbb{H}_b(\epsilon_n)}{(1-\epsilon_n)\sqrt{n \sum_z \frac{\left(1-\xi^{(n)}(z)\right)}{2Q_\emptyset(z)} \sum_{j=1}^n \left(\Psi_j^{(n)}(z)\right)^2}} \tag{3.105}$$

$$\leqslant \frac{\left(\sum_{i\in\mathcal{K}} \sum_{j=1}^n \mu_{ij}^{(n)}\right)\left(\mathbb{D}(P_k \| P_\emptyset) \frac{\sum_{j=1}^n \mu_{kj}^{(n)}}{\sum_{i\in\mathcal{K}} \sum_{j=1}^n \mu_{ij}^{(n)}} + d_4 \mu_{\max}^{(n)} + \frac{\mathbb{H}_b(\epsilon_n)}{\sum_{i\in\mathcal{K}} \sum_{j=1}^n \mu_{ij}^{(n)}}\right)}{(1-\epsilon_n)\sqrt{n \sum_z \frac{\left(1-\xi^{(n)}(z)\right)}{2Q_\emptyset(z)} \sum_{j=1}^n \left(\Psi_j^{(n)}(z)\right)^2}} \tag{3.106}$$

$$= \frac{\mathbb{D}(P_k \| P_\emptyset) \frac{\sum_{j=1}^n \mu_{kj}^{(n)}}{\sum_{i\in\mathcal{K}} \sum_{j=1}^n \mu_{ij}^{(n)}} + d_4 \mu_{\max}^{(n)} + \frac{\mathbb{H}_b(\epsilon_n)}{\sum_{i\in\mathcal{K}} \sum_{j=1}^n \mu_{ij}^{(n)}}}{(1-\epsilon_n)\sqrt{n \sum_z \frac{\left(1-\xi^{(n)}(z)\right)}{2Q_\emptyset(z)} \frac{\sum_{j=1}^n \left(\Psi_j^{(n)}(z)\right)^2}{\left(\sum_{i\in\mathcal{K}} \sum_{j=1}^n \mu_{ij}^{(n)}\right)^2}}}, \tag{3.107}$$

$$\overset{(a)}{\leqslant} \frac{\mathbb{D}(P_k \| P_\emptyset) \frac{\sum_{j=1}^n \mu_{kj}^{(n)}}{\sum_{i\in\mathcal{K}} \sum_{j=1}^n \mu_{ij}^{(n)}} + d_4 \mu_{\max}^{(n)} + \frac{\mathbb{H}_b(\epsilon_n)}{\sum_{i\in\mathcal{K}} \sum_{j=1}^n \mu_{ij}^{(n)}}}{(1-\epsilon_n)\sqrt{\sum_z \frac{\left(1-\xi^{(n)}(z)\right)}{2Q_\emptyset(z)} \left(\frac{\sum_{j=1}^n \Psi_j^{(n)}(z)}{\sum_{i\in\mathcal{K}} \sum_{j=1}^n \mu_{ij}^{(n)}}\right)^2}}, \tag{3.108}$$

where (a) follows from the fact that $n \sum_{j=1}^n \left(\Psi_j^{(n)}(z)\right)^2 \geqslant \left(\sum_{j=1}^n \Psi_j^{(n)}(z)\right)^2$ according to the Cauchy-Schwarz inequality. Note that since $\left(1-\xi^{(n)}(z)\right)$ is positive for n large enough, our application of Cauchy-Schwarz inequality in (3.108) is valid. From the definition of $\Psi_j^{(n)}(z)$ in (3.61), we have

$$\Psi_j^{(n)}(z) = \sum_{i\in\mathcal{K}} \mu_{ij}^{(n)} G_i(z) + \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ |\mathcal{T}|\geqslant 2}} \left(\prod_{k\in\mathcal{T}} \mu_{kj}^{(n)}\right) G_{\mathcal{T}}(z) \tag{3.109}$$

$$= \sum_{i\in\mathcal{K}} \left(\mu_{ij}^{(n)} G_i(z) + \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ i\in\mathcal{T}, |\mathcal{T}|\geqslant 2,\\ \forall k\in\mathcal{T}, k\geqslant i}} \mu_{ij}^{(n)} \left(\prod_{k\in\mathcal{T}\setminus\{i\}} \mu_{kj}^{(n)}\right) G_{\mathcal{T}}(z) \right) \tag{3.110}$$

$$= \sum_{i\in\mathcal{K}} \mu_{ij}^{(n)} \left(G_i(z) + \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ i\in\mathcal{T},|\mathcal{T}|\geqslant 2,\\ \forall k\in\mathcal{T},k\geqslant i}} \left(\prod_{k\in\mathcal{T}\setminus\{i\}} \mu_{kj}^{(n)} \right) G_{\mathcal{T}}(z) \right). \tag{3.111}$$

Define $d_5 \triangleq 2^K \max\limits_{z\in\mathcal{Z}} \max\limits_{\mathcal{T}\subseteq\mathcal{K}:|\mathcal{T}|>1} |G_{\mathcal{T}}(z)|$. If $\sum_{i\in\mathcal{K}} \mu_{ij}^{(n)} G_i(z) \leqslant 0$, we upper bound (3.111) by

$$\Psi_j^{(n)}(z) \leqslant \sum_{i\in\mathcal{K}} \mu_{ij}^{(n)} \left(G_i(z) + d_5 \mu_{\max}^{(n)} \right), \tag{3.112}$$

which is negative for n large enough. If $\sum_{i\in\mathcal{K}} \mu_{ij}^{(n)} G_i(z) \geqslant 0$, we lower bound (3.111) by

$$\Psi_j^{(n)}(z) \geqslant \sum_{i\in\mathcal{K}} \mu_{ij}^{(n)} \left(G_i(z) - d_5 \mu_{\max}^{(n)} \right), \tag{3.113}$$

which is positive for n large enough. Consequently, combining (3.108), (3.112) and (3.113) for n large enough, we obtain

$$\frac{\log M_k}{\sqrt{n\delta_n}} \leqslant \frac{\mathbb{D}(P_k\|P_\emptyset) \frac{\sum_{j=1}^n \mu_{kj}^{(n)}}{\sum_{i\in\mathcal{K}}\sum_{j=1}^n \mu_{ij}^{(n)}} + d_4 \mu_{\max}^{(n)} + \frac{\mathbb{H}_b(\epsilon_n)}{\sum_{i\in\mathcal{K}}\sum_{j=1}^n \mu_{ij}^{(n)}}}{(1-\epsilon_n)\sqrt{\sum_z \frac{\left(1-\xi^{(n)}(z)\right)}{2Q_\emptyset(z)} \left(\frac{\sum_{j=1}^n \Psi_j^{(n)}(z)}{\sum_{i\in\mathcal{K}}\sum_{j=1}^n \mu_{ij}^{(n)}} \right)^2}} \tag{3.114}$$

$$= \frac{\mathbb{D}(P_k\|P_\emptyset) \frac{\sum_{j=1}^n \mu_{kj}^{(n)}}{\sum_{i\in\mathcal{K}}\sum_{j=1}^n \mu_{ij}^{(n)}} + d_4 \mu_{\max}^{(n)} + \frac{\mathbb{H}_b(\epsilon_n)}{\sum_{i\in\mathcal{K}}\sum_{j=1}^n \mu_{ij}^{(n)}}}{(1-\epsilon_n)\sqrt{\sum_z \frac{\left(1-\xi^{(n)}(z)\right)}{2Q_\emptyset(z)} \left(\frac{\sum_{a\in\mathcal{K}} \left(G_a(z) + \mathcal{O}\left(\mu_{\max}^{(n)}\right) \right) \sum_{j=1}^n \mu_{aj}^{(n)}}{\sum_{i\in\mathcal{K}}\sum_{j=1}^n \mu_{ij}^{(n)}} \right)^2}}. \tag{3.115}$$

Combining (3.86) and (3.104) with the fact that $\lim\limits_{\substack{n\to\infty\\ n\in\mathcal{N}^*}} \log M_k = \infty$, we conclude that $\lim\limits_{\substack{n\to\infty\\ n\in\mathcal{N}^*}} \sum_{i\in\mathcal{K}}\sum_{j=1}^n \mu_{ij}^{(n)} = \infty$. Note that $\frac{\sum_{j=1}^n \mu_{aj}^{(n)}}{\sum_{i\in\mathcal{K}}\sum_{j=1}^n \mu_{ij}^{(n)}}$ is bounded between 0 and 1 for any $a \in \mathcal{K}$. We extract a convergent subsequence $\left\{ \frac{\sum_{j=1}^n \mu_{aj}^{(n)}}{\sum_{i\in\mathcal{K}}\sum_{j=1}^n \mu_{ij}^{(n)}} \right\}_{n\in\mathcal{N}^\dagger}$, where $\mathcal{N}^\dagger \subseteq \mathcal{N}^*$ is an infinite set, with limit ρ_a. Note that $\sum_{a\in\mathcal{K}} \rho_a = 1$. Since we have

assumed in Section 3.3 that there exists no $\{\rho_k\}_{k\in\mathcal{K}}$ for which $\sum_{k\in\mathcal{K}}\rho_k Q_k(z) = Q_\emptyset(z)$ for all $z \in \mathcal{Z}$, the denominator in (3.115) is non-zero. Henceforth, we only consider the subsequence of codes with blocklength $n \in \mathcal{N}^\dagger$. Defining $\boldsymbol{\rho} \triangleq \{\rho_k\}_{k\in\mathcal{K}}$, we obtain from (3.115),

$$\liminf_{\substack{n\to\infty \\ n\in\mathcal{N}^\dagger}} \frac{\log M_k}{\sqrt{n\delta_n}} \leqslant \sqrt{2}\rho_k \frac{\mathbb{D}(P_k\|P_\emptyset)}{\sqrt{\sum_z \frac{\left(\sum_{i\in\mathcal{K}}\rho_i(Q_i(z)-Q_\emptyset(z))\right)^2}{Q_\emptyset(z)}}} \tag{3.116}$$

$$\stackrel{(a)}{=} \sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k \mathbb{D}(P_k\|P_\emptyset), \tag{3.117}$$

where (a) follows from the definition of $\chi(\boldsymbol{\rho})$.

Using standard techniques, we lower bound $\log M_k L_k$, for $k \in \mathcal{K}$, by

$$\log M_k L_k = \mathbb{H}(W_k S_k) \tag{3.118}$$

$$\geqslant \mathbb{I}(W_k S_k; \mathbf{Z}) \tag{3.119}$$

$$\stackrel{(a)}{=} \mathbb{I}(\mathbf{X}_k; \mathbf{Z}) \tag{3.120}$$

$$= \mathbb{I}(\mathbf{X}[\mathcal{K}]; \mathbf{Z}) - \mathbb{I}(\mathbf{X}\left[\mathcal{K}\setminus\{k\}\right]; \mathbf{Z}|\mathbf{X}_k), \tag{3.121}$$

where (a) follows from the fact that $\mathbf{X}_k$ is a function of W_k and S_k. Defining $d_6 \triangleq$

$2^K \max_{i\in\mathcal{K}} \mathbb{D}(Q_i\|Q_\emptyset)$, we then lower bound the first term in (3.121) by

$$\mathbb{I}(\mathbf{X}[\mathcal{K}];\mathbf{Z}) = \sum_{\mathbf{x}[\mathcal{K}]}\sum_{\mathbf{z}}\left(\prod_{i\in\mathcal{K}}\Pi_{X_i}^n(\mathbf{x}_i)\right) W_{Z|X[\mathcal{K}]}^{\otimes n}(\mathbf{z}|\mathbf{x}[\mathcal{K}])\log\frac{W_{Z|X[\mathcal{K}]}^{\otimes n}(\mathbf{z}|\mathbf{x}[\mathcal{K}])}{\widehat{Q}^n(\mathbf{z})} \tag{3.122}$$

$$= \sum_{\mathbf{x}[\mathcal{K}]}\sum_{\mathbf{z}}\left(\prod_{i\in\mathcal{K}}\Pi_{X_i}^n(\mathbf{x}_i)\right) W_{Z|X[\mathcal{K}]}^{\otimes n}(\mathbf{z}|\mathbf{x}[\mathcal{K}])\log\frac{W_{Z|X[\mathcal{K}]}^{\otimes n}(\mathbf{z}|\mathbf{x}[\mathcal{K}])}{Q_\emptyset^{\otimes n}(\mathbf{z})} - \delta_n \tag{3.123}$$

$$= \sum_{j=1}^n \sum_{x_{(j)}[\mathcal{K}]}\sum_{z}\left(\prod_{i\in\mathcal{K}}\Pi_{X_{ij}}(x_{ij})\right) W_{Z|X[\mathcal{K}]}(z|x_{(j)}[\mathcal{K}])\log\frac{W_{Z|X[\mathcal{K}]}(z|x_{(j)}[\mathcal{K}])}{Q_\emptyset(z)} - \delta_n \tag{3.124}$$

$$= \sum_{j=1}^n \sum_{\mathcal{T}\subseteq\mathcal{K}}\left(\prod_{i\in\mathcal{T}}\mu_{ij}^{(n)}\right)\left(\prod_{i\in\mathcal{T}^c}\left(1-\mu_{ij}^{(n)}\right)\right)\mathbb{D}(Q_\mathcal{T}\|Q_\emptyset) - \delta_n \tag{3.125}$$

$$\geqslant \sum_{j=1}^n \sum_{i\in\mathcal{K}}\mu_{ij}^{(n)}\left(\prod_{i'\in\mathcal{K}\setminus\{i\}}\left(1-\mu_{i'j}^{(n)}\right)\right)\mathbb{D}(Q_i\|Q_\emptyset) - \delta_n \tag{3.126}$$

$$\overset{(a)}{\geqslant} \sum_{j=1}^n \sum_{i\in\mathcal{K}}\mu_{ij}^{(n)}\mathbb{D}(Q_i\|Q_\emptyset) - d_6\mu_{\max}^{(n)}\sum_{i\in\mathcal{K}}\sum_{j=1}^n\mu_{ij}^{(n)} - \delta_n, \tag{3.127}$$

where (a) follows from the steps used to obtain (3.98) from (3.94). Note that, by definition, we have

$$\sum_{\mathcal{T}\subseteq\mathcal{K}\setminus\{k\}}\left(\prod_{i\in\mathcal{K}\setminus\{k\}}\Pi_{X_{ij}}(x_{\mathcal{T},i})\right) W_{Z_j|X_{(j)}[\mathcal{K}\setminus\{k\}]X_{kj}}(z|x_\mathcal{T}[\mathcal{K}\setminus\{k\}]x) = W_{Z_j|X_{kj}}(z|x). \tag{3.128}$$

We upper bound the second term in (3.121) by

$$
\begin{aligned}
&\mathbb{I}(\mathbf{X}\left[\mathcal{K}\setminus\{k\}\right];\mathbf{Z}|\mathbf{X}_k)\\
&\quad=\mathbb{H}(\mathbf{Z}|\mathbf{X}_k)-\mathbb{H}(\mathbf{Z}|\mathbf{X}[\mathcal{K}]) && (3.129)\\
&\quad\overset{(a)}{\leqslant}\sum_{j=1}^{n}\big(\mathbb{H}(Z_j|X_{kj})-\mathbb{H}\big(Z_j|X_{(j)}[\mathcal{K}]\big)\big) && (3.130)\\
&\quad=\sum_{j=1}^{n}\mathbb{I}\big(X_{(j)}[\mathcal{K}\setminus\{k\}];Z_j|X_{kj}\big) && (3.131)\\
&\quad=\sum_{j=1}^{n}\sum_{\mathcal{T}\subseteq\mathcal{K}}\left(\prod_{i\in\mathcal{K}}\Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right)\mathbb{D}\big(Q_{\mathcal{T}}\|W_{Z_j|X_{kj}=x_{\mathcal{T},k}}\big) && (3.132)\\
&\quad=\sum_{j=1}^{n}\sum_{\mathcal{T}\subseteq\mathcal{K}}\left(\prod_{i\in\mathcal{K}}\Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right)\mathbb{D}(Q_{\mathcal{T}}\|Q_{\emptyset})\\
&\qquad-\sum_{j=1}^{n}\sum_{\mathcal{T}\subseteq\mathcal{K}}\left(\prod_{i\in\mathcal{K}}\Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right)\sum_{z}Q_{\mathcal{T}}(z)\log\frac{W_{Z_j|X_{kj}}\left(z|x_{\mathcal{T},k}\right)}{Q_{\emptyset}(z)} && (3.133)\\
&\quad=\sum_{j=1}^{n}\sum_{\mathcal{T}\subseteq\mathcal{K}}\left(\prod_{i\in\mathcal{K}}\Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right)\mathbb{D}(Q_{\mathcal{T}}\|Q_{\emptyset})\\
&\qquad-\sum_{j=1}^{n}\sum_{x}\Pi_{X_{kj}}(x)\sum_{z}\sum_{\mathcal{T}\subseteq\mathcal{K}\setminus\{k\}}\left(\prod_{i\in\mathcal{K}\setminus\{k\}}\Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right)\\
&\qquad\quad\times W_{Z_j|X_{(j)}[\mathcal{K}\setminus\{k\}]X_{kj}}\left(z|x_{\mathcal{T}}[\mathcal{K}\setminus\{k\}]x\right)\log\frac{W_{Z_j|X_{kj}}\left(z|x\right)}{Q_{\emptyset}(z)} && (3.134)\\
&\quad\overset{(b)}{=}\sum_{j=1}^{n}\sum_{\mathcal{T}\subseteq\mathcal{K}}\left(\prod_{i\in\mathcal{K}}\Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right)\mathbb{D}(Q_{\mathcal{T}}\|Q_{\emptyset})-\sum_{j=1}^{n}\sum_{x}\Pi_{X_{kj}}(x)\mathbb{D}\big(W_{Z_j|X_{kj}=x}\|Q_{\emptyset}\big) && (3.135)\\
&\quad\leqslant\sum_{j=1}^{n}\sum_{\mathcal{T}\subseteq\mathcal{K}}\left(\prod_{i\in\mathcal{K}}\Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right)\mathbb{D}(Q_{\mathcal{T}}\|Q_{\emptyset})-\sum_{j=1}^{n}\mu_{kj}^{(n)}\mathbb{D}\big(W_{Z_j|X_{kj}=1}\|Q_{\emptyset}\big), && (3.136)
\end{aligned}
$$

where (a) follows from the fact that conditioning reduces entropy and the memoryless property of the channel, and (b) follows from (3.128). Define $d_7 \triangleq 2^K \max\limits_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ |\mathcal{T}|>1}} \mathbb{D}(Q_{\mathcal{T}}\|Q_{\emptyset})$.

Then, we upper bound the first term in (3.136) by

$$\begin{aligned}
&\sum_{j=1}^{n}\sum_{\mathcal{T}\subseteq\mathcal{K}}\left(\prod_{i\in\mathcal{K}}\Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right)\mathbb{D}(Q_{\mathcal{T}}\|Q_{\emptyset})\\
&=\sum_{j=1}^{n}\sum_{\mathcal{T}\subseteq\mathcal{K}}\left(\prod_{i\in\mathcal{T}}\mu_{ij}^{(n)}\right)\left(\prod_{i\in\mathcal{T}^c}\left(1-\mu_{ij}^{(n)}\right)\right)\mathbb{D}(Q_{\mathcal{T}}\|Q_{\emptyset}) &(3.137)\\
&\overset{(a)}{\leqslant}\sum_{j=1}^{n}\sum_{\mathcal{T}\subseteq\mathcal{K}}\left(\prod_{i\in\mathcal{T}}\mu_{ij}^{(n)}\right)\mathbb{D}(Q_{\mathcal{T}}\|Q_{\emptyset}) &(3.138)\\
&=\sum_{j=1}^{n}\sum_{i\in\mathcal{K}}\mu_{ij}^{(n)}\mathbb{D}(Q_i\|Q_{\emptyset})+\sum_{j=1}^{n}\sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\|\mathcal{T}|>1}}\left(\prod_{i\in\mathcal{T}}\mu_{ij}^{(n)}\right)\mathbb{D}(Q_{\mathcal{T}}\|Q_{\emptyset}) &(3.139)\\
&\leqslant\sum_{j=1}^{n}\sum_{i\in\mathcal{K}}\mu_{ij}^{(n)}\mathbb{D}(Q_i\|Q_{\emptyset})+d_7\mu_{\max}^{(n)}\sum_{i\in\mathcal{K}}\sum_{j=1}^{n}\mu_{ij}^{(n)}, &(3.140)
\end{aligned}$$

where (a) follows from the fact that $\left(\prod_{i\in\mathcal{T}^c}\left(1-\mu_{ij}^{(n)}\right)\right)\leqslant 1$ for any $\mathcal{T}\subseteq\mathcal{K}$. Then, from Corollary 1, we write

$$W_{Z_j|X_{kj}}(z|1)=Q_k(z)+\sum_{\substack{\mathcal{T}\subseteq\mathcal{K}\setminus\{k\}:\\\mathcal{T}\neq\emptyset}}\left(\prod_{i\in\mathcal{T}}\mu_{ij}^{(n)}\right)\left(\sum_{\mathcal{U}\subseteq\mathcal{T}}(-1)^{|\mathcal{T}|-|\mathcal{U}|}\,Q_{\mathcal{U}\cup\{k\}}(z)\right). \quad (3.141)$$

Defining $d_8\triangleq 2^K\max\limits_{\mathcal{T}\subseteq\mathcal{K}\setminus\{k\}:\mathcal{T}\neq\emptyset}\left|\sum_z\sum\limits_{\mathcal{U}\subseteq\mathcal{T}}(-1)^{|\mathcal{T}|-|\mathcal{U}|}\,Q_{\mathcal{U}\cup\{k\}}(z)\log\frac{Q_k(z)}{Q_\emptyset(z)}\right|$ and using (3.141),

we bound the second KL divergence term in (3.136) by

$$\begin{aligned}
&\mathbb{D}\big(W_{Z_j|X_{kj}=1}\|Q_\emptyset\big) \\
&\quad= \mathbb{D}\big(W_{Z_j|X_{kj}=1}\|Q_k\big) + \sum_z W_{Z_j|X_{kj}}(z|1)\log\frac{Q_k(z)}{Q_\emptyset(z)} && (3.142)\\
&\quad\geqslant \sum_z \left(Q_k(z) + \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}\setminus\{k\}:\\ \mathcal{T}\neq\emptyset}} \left(\prod_{i\in\mathcal{T}}\mu_{ij}^{(n)}\right)\left(\sum_{\mathcal{U}\subseteq\mathcal{T}}(-1)^{|\mathcal{T}|-|\mathcal{U}|}\,Q_{\mathcal{U}\cup\{k\}}(z)\right)\right)\log\frac{Q_k(z)}{Q_\emptyset(z)} && (3.143)\\
&\quad\geqslant \mathbb{D}(Q_k\|Q_\emptyset) - \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}\setminus\{k\}:\\ \mathcal{T}\neq\emptyset}} \left(\prod_{i\in\mathcal{T}}\mu_{ij}^{(n)}\right)\left|\sum_z\left(\sum_{\mathcal{U}\subseteq\mathcal{T}}(-1)^{|\mathcal{T}|-|\mathcal{U}|}\,Q_{\mathcal{U}\cup\{k\}}(z)\right)\log\frac{Q_k(z)}{Q_\emptyset(z)}\right| && (3.144)\\
&\quad\geqslant \mathbb{D}(Q_k\|Q_\emptyset) - d_8\mu_{\max}^{(n)}. && (3.145)
\end{aligned}$$

Defining $d_9 \triangleq d_7 + d_8$ and combining (3.136), (3.140), and (3.145), we obtain

$$\begin{aligned}
\mathbb{I}(\mathbf{X}\left[\mathcal{K}\setminus\{k\}\right];\mathbf{Z}|\mathbf{X}_k) &\leqslant \sum_{j=1}^n\sum_{i\in\mathcal{K}\setminus\{k\}}\mu_{ij}^{(n)}\mathbb{D}(Q_i\|Q_\emptyset) + d_7\mu_{\max}^{(n)}\sum_{i\in\mathcal{K}}\sum_{j=1}^n\mu_{ij}^{(n)} \\
&\quad + d_8\mu_{\max}^{(n)}\sum_{j=1}^n\mu_{kj}^{(n)} && (3.146)\\
&\leqslant \sum_{j=1}^n\sum_{i\in\mathcal{K}\setminus\{k\}}\mu_{ij}^{(n)}\mathbb{D}(Q_i\|Q_\emptyset) + d_9\mu_{\max}^{(n)}\sum_{i\in\mathcal{K}}\sum_{j=1}^n\mu_{ij}^{(n)}. && (3.147)
\end{aligned}$$

Defining $d_{10} \triangleq d_6 + d_9$ and combining (3.127) and (3.147), we bound (3.121) by

$$\log M_k L_k \geqslant \left(\sum_{j=1}^n\mu_{kj}^{(n)}\right)\mathbb{D}(Q_k\|Q_\emptyset) - d_{10}\mu_{\max}^{(n)}\sum_{i\in\mathcal{K}}\sum_{j=1}^n\mu_{ij}^{(n)} - \delta_n. \tag{3.148}$$

Normalizing $\log M_k L_k$, where $k \in \mathcal{K}$, by $\sqrt{n\delta_n}$, we obtain

$$\frac{\log M_k L_k}{\sqrt{n\delta_n}} \geqslant \frac{\left(\sum_{j=1}^{n} \mu_{kj}^{(n)}\right) \mathbb{D}(Q_k \| Q_\emptyset) - d_{10}\mu_{\max}^{(n)} \sum_{i\in\mathcal{K}} \sum_{j=1}^{n} \mu_{ij}^{(n)} - \delta_n}{\sqrt{n\delta_n}} \tag{3.149}$$

$$= \frac{\left(\sum_{j=1}^{n} \mu_{kj}^{(n)}\right) \left(\mathbb{D}(Q_k \| Q_\emptyset) - d_{10}\mu_{\max}^{(n)} \sum_{i\in\mathcal{K}} \frac{\sum_{j=1}^{n} \mu_{ij}^{(n)}}{\sum_{j=1}^{n} \mu_{kj}^{(n)}} - \frac{\delta_n}{\sum_{j=1}^{n} \mu_{kj}^{(n)}}\right)}{\sqrt{n\delta_n}}. \tag{3.150}$$

Consider a sequence of codes for which (3.117) holds with equality for all $k \in \mathcal{K}$. Proposition 1 confirms the existence of such schemes. As a result, for an arbitrary $\xi > 0$, we have

$$\liminf_{\substack{n\to\infty \\ n\in\mathcal{N}^\dagger}} \frac{\log M_k}{\sqrt{n\delta_n}} \geqslant (1-\xi)\sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k \mathbb{D}(P_k \| P_\emptyset). \tag{3.151}$$

Then, for that sequence of codes, using (3.86) and (3.104), we obtain

$$\liminf_{\substack{n\to\infty \\ n\in\mathcal{N}^\dagger}} \frac{\left(\sum_{j=1}^{n} \mu_{kj}^{(n)}\right) \mathbb{D}(P_k \| P_\emptyset) + d_4\mu_{\max}^{(n)} \sum_{i\in\mathcal{K}} \left(\sum_{j=1}^{n} \mu_{ij}^{(n)}\right) + \mathbb{H}_b(\epsilon_n)}{(1-\epsilon_n)\sqrt{n\delta_n}}$$

$$\geqslant (1-\xi)\sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k \mathbb{D}(P_k \| P_\emptyset). \tag{3.152}$$

On simplifying (3.152) further, we obtain

$$\liminf_{\substack{n\to\infty \\ n\in\mathcal{N}^\dagger}} \frac{\left(\sum_{j=1}^{n} \mu_{kj}^{(n)}\right) \left(\mathbb{D}(P_k \| P_\emptyset) + d_4\mu_{\max}^{(n)} \sum_{i\in\mathcal{K}} \frac{\sum_{j=1}^{n} \mu_{ij}^{(n)}}{\sum_{j=1}^{n} \mu_{kj}^{(n)}}\right)}{(1-\epsilon_n)\sqrt{n\delta_n}} \geqslant (1-\xi)\sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k \mathbb{D}(P_k \| P_\emptyset), \tag{3.153}$$

$$\liminf_{\substack{n\to\infty\\ n\in\mathcal{N}^\dagger}} \frac{\left(\sum_{j=1}^{n}\mu_{kj}^{(n)}\right)\mathbb{D}(P_k\|P_\emptyset)}{\sqrt{n\delta_n}} \geqslant (1-\xi)\sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k\mathbb{D}(P_k\|P_\emptyset), \tag{3.154}$$

$$\liminf_{\substack{n\to\infty\\ n\in\mathcal{N}^\dagger}} \frac{\sum_{j=1}^{n}\mu_{kj}^{(n)}}{\sqrt{n\delta_n}} \geqslant (1-\xi)\sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k. \tag{3.155}$$

However, since $\limsup_{n\to\infty} a_n \geqslant \liminf_{n\to\infty} a_n$ for any sequence $\{a_n\}$, we write

$$\limsup_{\substack{n\to\infty\\ n\in\mathcal{N}^\dagger}} \frac{\sum_{j=1}^{n}\mu_{kj}^{(n)}}{\sqrt{n\delta_n}} \geqslant (1-\xi)\sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k. \tag{3.156}$$

Combining (3.150) and (3.156), we obtain

$$\limsup_{\substack{n\to\infty\\ n\in\mathcal{N}^\dagger}} \frac{\log M_k L_k}{\sqrt{n\delta_n}} \geqslant (1-\xi)\sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k\mathbb{D}(Q_k\|Q_\emptyset), \tag{3.157}$$

for an arbitrary $\xi > 0$, where (a) follows from the fact that $\lim_{\substack{n\to\infty\\ n\in\mathcal{N}^\dagger}} \sum_{j=1}^{n}\mu_{kj}^{(n)} = \infty$. Letting $\xi \downarrow 0$ in (3.157), we obtain (3.41). □

Note that for any sequence $\{a_n\}_{n\in\mathbb{N}^*}$ and any infinite set $\mathcal{N} \subseteq \mathbb{N}^*$, we have, by definition,

$$\liminf_{n\to\infty} a_n \leqslant \liminf_{\substack{n\to\infty\\ n\in\mathcal{N}}} a_n \leqslant \limsup_{\substack{n\to\infty\\ n\in\mathcal{N}}} a_n \leqslant \limsup_{n\to\infty} a_n. \tag{3.158}$$

From Proposition 2 and equation (3.158), we conclude that the covert capacity region is contained in the region defined by

$$\bigcup_{\{\rho_k\}_{k\in\mathcal{K}}\in[0,1]^K:\sum_{k\in\mathcal{K}}\rho_k=1} \left\{ \{r_k\}_{k\in\mathcal{K}} : \forall k\in\mathcal{K}, \quad r_k \leqslant \sqrt{\frac{2}{\chi\left(\boldsymbol{\rho}\right)}}\rho_k\mathbb{D}(P_k\|P_\emptyset) \right\}, \tag{3.159}$$

and that, any achievable covert throughput tuple $r\left[\mathcal{K}\right]$ characterized by a specific $\boldsymbol{\rho}$ and lying on the boundary of the region defined in (3.159) is associated to an achiev-

able key throughput of at least $\sqrt{\frac{2}{\chi(\boldsymbol{\rho})}}\rho_k \left[\mathbb{D}(Q_k\|Q_\emptyset) - \mathbb{D}(P_k\|P_\emptyset)\right]^+$ for each $k \in \mathcal{K}$. The main reason why we need to resort to this approach is because, unlike traditional converse proofs, we require some statement about the limit of $\mu_{k1}^{(n)}$, which is a much more precise statement about the structure of the code than usually required. Traditional converse proofs single-letterize quantities such as entropy, mutual information, without having to make explicit statements about the distribution induced by the code. Part of the challenge is that it is not obvious *a priori* that quantities such as μ_{k1} behave nicely and our proof requires us to make statements about the limiting behavior of these quantities. In essence, our approach is a way of only focusing on "well-behaved codes" in the sequence. Mathematically, our approach is justified by properties of lim inf and lim sup.

3.6 Conclusion

We conclude with a discussion of extensions of our results and related problems of interest. Although we have limited our characterization of the covert capacity region to binary-input K-user MACs, our results also extend to transmitters with non-binary input alphabets as in [27, 33]. To be more specific, each user is now characterized by a distinct input alphabet $\mathcal{X}_k \triangleq [\![0, N_k]\!]$ with one innocent symbol 0 and N_k information symbols. The input distributions defined earlier in the chapter need to be suitably modified as follows.

$$\Pi_{X_k}(0) = 1 - \rho_k\alpha_n, \forall k \text{ and} \tag{3.160}$$

$$\Pi_{X_k}(i) = \rho_k\beta_{k,i}\alpha_n, \text{ for } i \in [\![1, N_k]\!], \tag{3.161}$$

where $\sum_{i\in[\![1,N_k]\!]}\beta_{k,i}=1$. We need to introduce a new notation to describe the distributions induced by a fixed choice of input.

$$\forall \mathbf{x}\in\bigtimes_{i=1}^{K}\mathcal{X}_i \quad Q_{\mathbf{x}}(z)=W_{Z|X[\mathcal{K}]}(z|\mathbf{x}). \tag{3.162}$$

As done before, for a given vector $\mathbf{x}$, the vector $\mathbf{x}[\mathcal{T}]$ is the subvector of size $|\mathcal{T}|$ comprised of the components of $\mathbf{x}$ with index in $\mathcal{T}$. In addition $\mathbf{x}_{\mathcal{T}}=(x_{\mathcal{T},1},\ldots,x_{\mathcal{T},K})$ is a K length vector which contains the symbol 0 in positions indexed by $\mathcal{T}^c$. For $\mathcal{T}\subseteq\mathcal{K}$, we define the distributions

$$Q_{\mathcal{T}}(z)\triangleq\sum_{\mathbf{x}_{\mathcal{T}}}\left(\prod_{k\in\mathcal{T}}\beta_{k,x_{\mathcal{T},k}}\right)Q_{\mathbf{x}_{\mathcal{T}}}(z), \tag{3.163}$$

and

$$Q_{\alpha_n}(z)\triangleq\sum_{x[\mathcal{K}]}W_{Z|X[\mathcal{K}]}(z|x[\mathcal{K}])\left(\prod_{k\in\mathcal{K}}\Pi_{X_k}(x_k)\right). \tag{3.164}$$

In the special case that $\mathcal{T}$ is a singleton, say $\{k\}$, we simply write Q_k in place of $Q_{\mathcal{T}}$, and if the unique non-zero symbol in $\mathbf{x}_{\mathcal{T}}$ is $i\in[\![1,N_k]\!]$, we write $Q_{k,i}$ in place of $Q_{\mathbf{x}_{\mathcal{T}}}$. With this convention, note that we have

$$Q_k(z)=\sum_{i\in[\![1,N_k]\!]}\beta_{k,i}Q_{k,i}(z). \tag{3.165}$$

For $\boldsymbol{\rho}\in[0,1]^K$ and $\boldsymbol{\beta}\in[0,1]^K$, we finally introduce

$$\chi(\boldsymbol{\rho},\boldsymbol{\beta})=\sum_z\frac{\left(\sum_{k\in\mathcal{K}}\rho_k\left(Q_k(z)-Q_\emptyset(z)\right)\right)^2}{Q_\emptyset(z)} \tag{3.166}$$

$$=\sum_z\frac{\left(\sum_{k\in\mathcal{K}}\rho_k\left(\sum_{i\in[\![1,N_k]\!]}\beta_{k,i}Q_{k,i}(z)-Q_\emptyset(z)\right)\right)^2}{Q_\emptyset(z)}. \tag{3.167}$$

Similar notation holds when focusing on the main channel instead of the warden channel, in which case we write P instead of Q. With this notation, one can check that Lemma 1 may be extended to obtain

$$\frac{\alpha_n^2}{2}\left(1+\sqrt{\alpha_n}\right)\chi_n(\boldsymbol{\rho},\boldsymbol{\beta}) \geqslant \mathbb{D}(Q_{\alpha_n}\|Q_\emptyset) \geqslant \frac{\alpha_n^2}{2}\left(1-\sqrt{\alpha_n}\right)\chi_n(\boldsymbol{\rho},\boldsymbol{\beta}), \tag{3.168}$$

and

$$\mathbb{I}(X[\mathcal{T}];Z) = \alpha_n \sum_{k\in\mathcal{T}} \rho_k \sum_{i=1}^{N_k} \beta_{k,i}\mathbb{D}(Q_{k,i}\|Q_\emptyset) + \mathcal{O}\left(\alpha_n^2\right). \tag{3.169}$$

Notice that while $\chi(\boldsymbol{\rho})$ only depends on the distributions $\{Q_k\}_{k\in\mathcal{K}}$, the expansion of the mutual information involves distributions $\{Q_{k,i}\}$, which effectively forces us to keep track of the $\{\beta_{k,i}\}$. It is then not too painful to check that the covert capacity region contains the region defined by

$$\bigcup_{\substack{\{\rho_k\}_{k\in\mathcal{K}}\in[0,1]^K:\sum_{k\in\mathcal{K}}\rho_k=1 \\ \{\beta_{k,i}\}_{k\in[\![1,K]\!],i\in[\![1,N_k]\!]}:\forall k\{\beta_{k,i}\}_{i=1}^{N_k}\in[0,1]^{N_k},\sum_{i=1}^{N_k}\beta_{k,i}=1}} \left\{ \{r_k\}_{k\in\mathcal{K}} : \forall k\in\mathcal{K}, \right. \\ \left. r_k \leqslant \sqrt{\frac{2}{\chi\left(\boldsymbol{\rho},\boldsymbol{\beta}\right)}}\rho_k \sum_{i=1}^{N_k}\beta_{k,i}\mathbb{D}(P_{k,i}\|P_\emptyset) \right\}. \tag{3.170}$$

For the converse part, one can define

$$1-\mu_{kj}^{(n)} \triangleq \Pi_{X_{kj}}(0) \triangleq \frac{\sum_{m_k=1}^{M_k}\sum_{\ell_k=1}^{L_k}\mathbb{1}\{X_{kj}(m_k,\ell_k)=0\}}{M_kL_k}, \tag{3.171}$$

and for $i\in[\![1,N_k]\!]$

$$\Pi_{X_{kj}}(i) \triangleq \mu_{kj}^{(n)}\beta_{k,i,j}^{(n)}, \tag{3.172}$$

in which case the steps leading to the lower bound of the KL divergence are identical,

thanks to our redefinition of $Q_{\mathcal{T}}$ and Q_k done earlier. The steps leading to the upper bound of the mutual information require slightly more care because must be replaced by

$$\sum_{\mathcal{T}\subseteq\mathcal{K}}\sum_{\mathbf{x}_{\mathcal{T}}}\left(\prod_{i\in\mathcal{K}}\Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right)\mathbb{D}(P_{\mathbf{x}_{\mathcal{T}}}\|P_{\emptyset})$$
$$-\sum_{y}\sum_{\mathcal{T}\subseteq\mathcal{K}}\sum_{\mathbf{x}_{\mathcal{T}}}\left(\prod_{i\in\mathcal{K}}\Pi_{X_{ij}}\left(x_{\mathcal{T},i}\right)\right)P_{\mathbf{x}_{\mathcal{T}}}\left(y\right)\log\frac{W_{Y_j|X_{(j)}[\mathcal{K}\setminus\{k\}]}\left(y|x_{\mathcal{T}}\left[\mathcal{K}\setminus\{k\}\right]\right)}{P_{\emptyset}(y)}, \quad (3.173)$$

to account for multiple information symbols. Checking how this affects the remaining calculations requires additional care, but one can check that we obtain a modified version of (3.104) of the form

$$\mathbb{I}(X_{kj};Y_j|X_j\left[\mathcal{K}\setminus\{k\}\right])\leqslant\mu_{kj}^{(n)}\sum_{\ell=1}^{N_k}\beta_{i,\ell,j}^{(n)}\mathbb{D}(P_{k,\ell}\|P_{\emptyset})+d_4\mu_{\max}^{(n)}\sum_{i\in\mathcal{K}}\mu_{ij}^{(n)}\sum_{\ell=1}^{N_i}\beta_{i,\ell,j}^{(n)}. \quad (3.174)$$

Following the exact same steps earlier in the chapter, one obtains the converse matching the achievability region highlighted earlier. The analysis of the least achievable key rates on the boundary follows similarly.

Our results do extend to AWGN channels. If covertness were to be measured with variational distance and if one were to use on-off-keying, one could follow the approach outlined in [71] and handle the covert constraint as done in our achievability proof. However, since our results focus on KL divergence to measure covertness, an achievability proof must accommodate the continuous nature of the AWGN channel alphabet and possibly the need to use input distributions that are not discrete (see [33]). One solution is to use a resolvability exponent approach [72], [73], [74] instead of the typical-sequence approach used in this chapter to obtain bounds for the KL divergence $\mathbb{D}\big(\widehat{Q}^n\|Q_{\emptyset}^{\otimes n}\big)$ that do not depend on the alphabet cardinality. One technical aspect of this approach is that one must perform a careful Taylor series of the resolvability exponent. As for the converse part, one can follow the steps used

in [33] with the necessary adaptations to handle multiple users. More specifically, Following the single-letterization approach of [33], we obtain

$$\mathbb{D}\Big(\hat{Q}_n \| Q_0^{\otimes n}\Big) \geqslant \sum_{j=1}^{n} \mathbb{D}\Big(\hat{Q}_j \| Q_0\Big) \tag{3.14}$$

$$= \sum_{j=1}^{n} \left(-h(\hat{Q}_j^n) + \frac{1}{2}\log 2\pi\sigma^2 + \mathbb{E}\left([]\,\hat{Q}_j\right] \frac{Z^2}{2\sigma^2} \right) \tag{3.15}$$

Because Z_j and the channel inputs $\{X_{i,j}\}$ are independent (by definition), we have

$$\mathrm{Var}(Z) = \sigma^2 + \sum_{i \in \mathcal{K}} \underbrace{\mathrm{Var}(X_{i,j})}_{\triangleq \theta_{i,j}}. \tag{3.16}$$

Since a Gaussian distribution maximizes the differential entropy among all variables with the same variance and since the variance is a lower bound on the second order moment, we obtain

$$\mathbb{D}\Big(\hat{Q}_j \| Q_0\Big) \geqslant -\frac{1}{2}\log(2\pi e(\sigma^2 + \sum_{i \in \mathcal{K}} \theta_{i,j})) + \frac{1}{2}\log 2\pi\sigma^2 + \frac{\sigma^2 + \sum_{i \in \mathcal{K}} \theta_{i,j}}{2\sigma^2} \tag{3.17}$$

$$= \frac{\sum_{i \in \mathcal{K}} \theta_{i,j}}{2\sigma^2} - \frac{1}{2}\log\left(1 + \frac{\sum_{i \in \mathcal{K}} \theta_{i,j}}{\sigma^2}\right). \tag{3.18}$$

Since we can argue as done in this chapter that every $\sum_{i \in \mathcal{K}} \theta_{i,j}$ should vanish, we obtain

$$\mathbb{D}\Big(\hat{Q}_n \| Q_0^{\otimes n}\Big) \geqslant \sum_{j=1}^{n} \left(\frac{(\sum_{i \in \mathcal{K}} \theta_{i,j})^2}{4\sigma^4} + o\left((\sum_{i \in \mathcal{K}} \theta_{i,j})^2 \right) \right) \tag{3.19}$$

$$\geqslant \frac{1}{n} \left(\frac{(\sum_{i \in \mathcal{K}} \sum_{j=1}^{n} \theta_{i,j})^2}{4\sigma^4} + o\left((\sum_{i \in \mathcal{K}} \sum_{j=1}^{n} \theta_{i,j})^2 \right) \right). \tag{3.20}$$

Note that the last step should be argued a bit more carefully but is nevertheless

correct. Similarly, we can upper bound $\log M_k$ as

$$\log M_k \leqslant \frac{1}{1-\epsilon_n}\left(\sum_{j=1}^{n}\frac{1}{2}\log\left(1+\frac{\theta_{k,j}}{\sigma^2}\right)+H_b(\epsilon_n)\right) \tag{3.21}$$

$$\leqslant \frac{1}{1-\epsilon_n}\left(\sum_{j=1}^{n}\frac{\theta_{k,j}}{2\sigma^2}+H_b(\epsilon_n)\right) \tag{3.22}$$

Putting everything together, one would then obtain

$$\frac{\log M_k}{\sqrt{n\mathbb{D}\left(\hat{Q}_j\|Q_0\right)}} \leqslant \frac{\sum_{j=1}^{n}\frac{\theta_{k,j}}{2\sigma^2}+H_b(\epsilon_n)}{(1-\epsilon_n)\sqrt{\frac{(\sum_{i\in\mathcal{K}}\sum_{j=1}^{n}\theta_{i,j})^2}{4\sigma^4}+o\left((\sum_{i\in\mathcal{K}}\sum_{j=1}^{n}\theta_{i,j})^2\right)}} \tag{3.23}$$

$$= \frac{1}{(1-\epsilon_n)\sqrt{1+o(1))}}\left(\frac{\sum_{i=1}^{n}\theta_{k,i}}{\sum_{i\in\mathcal{K}}\sum_{j=1}^{n}\theta_{i,j}}+\frac{H_b(\epsilon_n)}{\sum_{i\in\mathcal{K}}\sum_{j=1}^{n}\theta_{i,j}}\right) \tag{3.24}$$

Reproducing the reasoning in this chapter to deal with all the terms properly, we would then obtain that the covert capacity must be contained in the region described by

$$\bigcup_{\{\rho_k\}_{k\in\mathcal{K}}:\sum_k\rho_k=1}\left\{\{r_k\}_{k\in\mathcal{K}}:r_k\leqslant\rho_k\right\}. \tag{3.25}$$

A final problem of interest is the characterization of the covert capacity region of a K-user MAC in which the transmitters share a *common* key. Unlike the situation addressed here, the common key scenario captures the ability of users to *coordinate* their covert transmissions. One can approach the problem by following cooperative channel resolvability techniques studied in [75, 76].

APPENDIX

3.A Alternative representation of Q_{α_n} in Eq. (3.11)

Lemma 6. *For any set $\mathcal{S} \subseteq \mathcal{K}$, define $G_{\mathcal{S}}(z) \triangleq \sum_{\mathcal{T} \subseteq \mathcal{S}} (-1)^{|\mathcal{S}|-|\mathcal{T}|} Q_{\mathcal{T}}(z)$. Then,*

$$Q_{\alpha_n}(z) = Q_{\emptyset}(z) + \sum_{\substack{\mathcal{S} \subseteq \mathcal{K}: \\ \mathcal{S} \neq \emptyset}} \left(\prod_{k \in \mathcal{S}} \rho_k \alpha_n \right) G_{\mathcal{S}}(z). \tag{3.26}$$

Proof. First, we prove the following statement by induction. For any set $\mathcal{S}$ and $\beta_k \in [0,1]$ for $k \in \mathcal{K}$,

$$\prod_{k \in \mathcal{S}} (1 - \beta_k) = 1 + \sum_{\substack{\mathcal{T} \subseteq \mathcal{S}: \\ \mathcal{T} \neq \emptyset}} (-1)^{|\mathcal{T}|} \left(\prod_{k \in \mathcal{T}} \beta_k \right). \tag{3.27}$$

It is straightforward to show that (3.27) is true for $\mathcal{S} = \{1\}$. When $\mathcal{S} = \{1, 2\}$, we have

$$\prod_{k \in \{1,2\}} (1 - \beta_k) = 1 + \sum_{\substack{\mathcal{T} \subseteq \{1,2\}: \\ \mathcal{T} \neq \emptyset}} (-1)^{|\mathcal{T}|} \left(\prod_{k \in \mathcal{T}} \beta_k \right) \tag{3.28}$$

$$= 1 - \beta_1 - \beta_2 + \beta_1 \beta_2. \tag{3.29}$$

We assume that (3.27) is true for the set $\mathcal{S} \triangleq [\![1, K-1]\!]$, where $K \in \mathbb{N}^*$. Then, for the set $\mathcal{S}' \triangleq \mathcal{S} \cup \{K\}$, we have

$$\prod_{k \in \mathcal{S}'} (1 - \beta_k) = (1 - \beta_K) \prod_{k \in \mathcal{S}} (1 - \beta_k) \tag{3.30}$$

$$= (1 - \beta_K) \left(1 + \sum_{\substack{\mathcal{T} \subseteq \mathcal{S}: \\ \mathcal{T} \neq \emptyset}} (-1)^{|\mathcal{T}|} \left(\prod_{k \in \mathcal{T}} \beta_k \right) \right) \tag{3.31}$$

$$= 1 - \beta_K + \sum_{\substack{\mathcal{T}\subseteq\mathcal{S}:\\ \mathcal{T}\neq\emptyset}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right) - \beta_K \left(\sum_{\substack{\mathcal{T}\subseteq\mathcal{S}:\\ \mathcal{T}\neq\emptyset}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right)\right) \tag{3.32}$$

$$\overset{(a)}{=} 1 + \sum_{\mathcal{T}=\{K\}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right) + \sum_{\substack{\mathcal{T}\subseteq\mathcal{S}:\\ |\mathcal{T}|=1}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right)$$
$$+ \sum_{\substack{\mathcal{T}\subseteq\mathcal{S}:\\ |\mathcal{T}|>1}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right) + \sum_{\substack{\mathcal{T}\subseteq\mathcal{S}':\\ |\mathcal{T}|>1,\ K\in\mathcal{T}}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right) \tag{3.33}$$

$$\overset{(b)}{=} 1 + \sum_{\substack{\mathcal{T}\subseteq\mathcal{S}':\\ |\mathcal{T}|=1}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right) + \sum_{\substack{\mathcal{T}\subseteq\mathcal{S}':\\ |\mathcal{T}|>1,\ K\notin\mathcal{T}}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right)$$
$$+ \sum_{\substack{\mathcal{T}\subseteq\mathcal{S}':\\ |\mathcal{T}|>1,\ K\in\mathcal{T}}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right) \tag{3.34}$$

$$= 1 + \sum_{\substack{\mathcal{T}\subseteq\mathcal{S}':\\ |\mathcal{T}|=1}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right) + \sum_{\substack{\mathcal{T}\subseteq\mathcal{S}':\\ |\mathcal{T}|>1}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right) \tag{3.35}$$

$$= 1 + \sum_{\substack{\mathcal{T}\subseteq\mathcal{S}':\\ \mathcal{T}\neq\emptyset}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right), \tag{3.36}$$

where (a) follows from the fact that

$$(-\beta_K) \left(\sum_{\substack{\mathcal{T}\subseteq\mathcal{S}:\\ \mathcal{T}\neq\emptyset}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right)\right) = \sum_{\substack{\mathcal{T}\subseteq\mathcal{S}':\\ |\mathcal{T}|>1,\ K\in\mathcal{T}}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right), \tag{3.37}$$

and (b) follows from the fact that

$$\sum_{\substack{\mathcal{T}\subseteq\mathcal{S}:\\ |\mathcal{T}|>1}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right) = \sum_{\substack{\mathcal{T}\subseteq\mathcal{S}':\\ |\mathcal{T}|>1,\ K\notin\mathcal{T}}} (-1)^{|\mathcal{T}|} \left(\prod_{k\in\mathcal{T}} \beta_k\right). \tag{3.38}$$

From the definition of Q_{α_n} in (3.8), we have

$$Q_{\alpha_n}(z) = \sum_{x[\mathcal{K}]} \left(\prod_{k \in \mathcal{K}} \Pi_{X_k}(x_k) \right) W_{Z|X[\mathcal{K}]}(z|x[\mathcal{K}]) \tag{3.39}$$

$$= \sum_{\mathcal{T} \subseteq \mathcal{K}} \left(\prod_{k \in \mathcal{T}} \rho_k \alpha_n \right) \left(\prod_{k \in \mathcal{T}^c} (1 - \rho_k \alpha_n) \right) Q_{\mathcal{T}}(z) \tag{3.40}$$

$$= \left(\prod_{k \in \mathcal{K}} (1 - \rho_k \alpha_n) \right) Q_{\emptyset}(z) + \sum_{\substack{\mathcal{T} \subseteq \mathcal{K}: \\ \mathcal{T} \neq \emptyset}} \left(\prod_{k \in \mathcal{T}} \rho_k \alpha_n \right) \left(\prod_{k \in \mathcal{T}^c} (1 - \rho_k \alpha_n) \right) Q_{\mathcal{T}}(z) \tag{3.41}$$

$$\stackrel{(a)}{=} \sum_{\substack{\mathcal{T} \subseteq \mathcal{K}: \\ \mathcal{T} \neq \emptyset}} \left(\prod_{k \in \mathcal{T}} \rho_k \alpha_n \right) \left(1 + \sum_{\substack{\mathcal{U} \subseteq \mathcal{T}^c: \\ \mathcal{U} \neq \emptyset}} (-1)^{|\mathcal{U}|} \left(\prod_{k \in \mathcal{U}} \rho_k \alpha_n \right) \right) Q_{\mathcal{T}}(z) + \left(\prod_{k \in \mathcal{K}} (1 - \rho_k \alpha_n) \right) Q_{\emptyset}(z) \tag{3.42}$$

$$= \sum_{\substack{\mathcal{T} \subseteq \mathcal{K}: \\ \mathcal{T} \neq \emptyset}} \left(\prod_{k \in \mathcal{T}} \rho_k \alpha_n \right) \left(\sum_{\mathcal{U} \subseteq \mathcal{T}^c} (-1)^{|\mathcal{U}|} \left(\prod_{k \in \mathcal{U}} \rho_k \alpha_n \right) \right) Q_{\mathcal{T}}(z) + \left(\prod_{k \in \mathcal{K}} (1 - \rho_k \alpha_n) \right) Q_{\emptyset}(z), \tag{3.43}$$

where (a) follows from (3.27). Since $\mathcal{T}$ and $\mathcal{U}$ are disjoint sets, it follows from (3.43)

that

$$Q_{\alpha_n}(z) = \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \left(\prod_{k\in\mathcal{T}} \rho_k\alpha_n\right) \left(\sum_{\substack{\mathcal{S}\subseteq\mathcal{K}:\\ \mathcal{T}\subseteq\mathcal{S}}} (-1)^{|\mathcal{S}|-|\mathcal{T}|} \left(\prod_{k\in(\mathcal{S}\setminus\mathcal{T})} \rho_k\alpha_n\right)\right) Q_{\mathcal{T}}(z)$$

$$+ \left(\prod_{k\in\mathcal{K}} (1-\rho_k\alpha_n)\right) Q_\emptyset(z) \tag{3.44}$$

$$\overset{(a)}{=} Q_\emptyset(z) + \sum_{\substack{\mathcal{S}\subseteq\mathcal{K}:\\ \mathcal{S}\neq\emptyset}} (-1)^{|\mathcal{S}|} \left(\prod_{k\in\mathcal{S}} \rho_k\alpha_n\right) Q_\emptyset(z)$$

$$+ \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \left(\sum_{\substack{\mathcal{S}\subseteq\mathcal{K}:\\ \mathcal{T}\subseteq\mathcal{S}}} (-1)^{|\mathcal{S}|-|\mathcal{T}|} \left(\prod_{k\in\mathcal{S}} \rho_k\alpha_n\right)\right) Q_{\mathcal{T}}(z) \tag{3.45}$$

$$= Q_\emptyset(z) + \sum_{\substack{\mathcal{S}\subseteq\mathcal{K}:\\ \mathcal{S}\neq\emptyset}} (-1)^{|\mathcal{S}|} \left(\prod_{k\in\mathcal{S}} \rho_k\alpha_n\right) Q_\emptyset(z)$$

$$+ \sum_{\substack{\mathcal{S}\subseteq\mathcal{K}:\\ \mathcal{S}\neq\emptyset}} \left(\prod_{k\in\mathcal{S}} \rho_k\alpha_n\right) \left(\sum_{\substack{\mathcal{T}\subseteq\mathcal{S}:\\ \mathcal{T}\neq\emptyset}} (-1)^{|\mathcal{S}|-|\mathcal{T}|} Q_{\mathcal{T}}(z)\right) \tag{3.46}$$

$$= Q_\emptyset(z) + \sum_{\substack{\mathcal{S}\subseteq\mathcal{K}:\\ \mathcal{S}\neq\emptyset}} \left(\prod_{k\in\mathcal{S}} \rho_k\alpha_n\right) \left(\sum_{\mathcal{T}\subseteq\mathcal{S}} (-1)^{|\mathcal{S}|-|\mathcal{T}|} Q_{\mathcal{T}}(z)\right), \tag{3.47}$$

where (a) follows from (3.27). Defining $G_{\mathcal{S}}(z) \triangleq \sum_{\mathcal{T}\subseteq\mathcal{S}} (-1)^{|\mathcal{S}|-|\mathcal{T}|} Q_{\mathcal{T}}(z)$, we obtain

$$Q_{\alpha_n}(z) = Q_\emptyset(z) + \sum_{\substack{\mathcal{S}\subseteq\mathcal{K}:\\ \mathcal{S}\neq\emptyset}} \left(\prod_{k\in\mathcal{S}} \rho_k\alpha_n\right) G_{\mathcal{S}}(z). \tag{3.48}$$

□

Corollary 1. *For any set $\mathcal{S}\subseteq\mathcal{K}$, define $G_{\mathcal{S}}(z) \triangleq \sum_{\mathcal{T}\subseteq\mathcal{S}} (-1)^{|\mathcal{S}|-|\mathcal{T}|} Q_{\mathcal{T}}(z)$. Then,*

$$W_{Z|X_k}(z|1) = Q_k(z) + \sum_{\substack{\mathcal{S}\subseteq\mathcal{K}\setminus\{k\}:\\ \mathcal{S}\neq\emptyset}} \left(\prod_{i\in\mathcal{S}} \rho_i\alpha_n\right) \left(\sum_{\mathcal{T}\subseteq\mathcal{S}} (-1)^{|\mathcal{S}|-|\mathcal{T}|} Q_{\mathcal{T}\cup\{k\}}(z)\right). \tag{3.49}$$

3.B Proof of Lemma 2

From the definition of $\mathbb{D}(Q_{\alpha_n}\|Q_\emptyset)$, we have

$$\mathbb{D}(Q_{\alpha_n}\|Q_\emptyset) = \sum_z Q_{\alpha_n}(z)\log\frac{Q_{\alpha_n}(z)}{Q_\emptyset(z)} \tag{3.50}$$

$$= \sum_z Q_\emptyset(z)\left(1+\frac{\alpha_n\zeta_n(z)}{Q_\emptyset(z)}\right)\log\left(1+\frac{\alpha_n\zeta_n(z)}{Q_\emptyset(z)}\right). \tag{3.51}$$

Since $\log(1+x) < x - \frac{x^2}{2} + \frac{x^3}{3}$, for $x > -1$, we upper bound (3.51) by

$$\mathbb{D}(Q_{\alpha_n}\|Q_\emptyset) \leqslant \sum_z Q_\emptyset(z)\left(1+\frac{\alpha_n\zeta_n(z)}{Q_\emptyset(z)}\right)\left(\frac{\alpha_n\zeta_n(z)}{Q_\emptyset(z)} - \frac{\alpha_n^2\zeta_n^2(z)}{2Q_\emptyset^2(z)} + \frac{\alpha_n^3\zeta_n^3(z)}{3Q_\emptyset^3(z)}\right) \tag{3.52}$$

$$\overset{(a)}{=} \sum_z \frac{\alpha_n^2}{2}\left(\frac{\zeta_n^2(z)}{Q_\emptyset(z)} - \frac{\alpha_n\zeta_n^3(z)}{3Q_\emptyset^2(z)} + \frac{2\alpha_n^2\zeta_n^4(z)}{3Q_\emptyset^3(z)}\right), \tag{3.53}$$

where, (a) follows from the fact that $\sum_z \zeta_n(z) = 0$ from the definition of ζ_n. Since $\lim_{n\to\infty}\alpha_n = 0$, α_n is small enough for a sufficiently large n and $\frac{\alpha_n\zeta_n(z)}{Q_\emptyset(z)} \in \left[-\frac{1}{2}, 0\right]$ for any $z \in \mathcal{Z}$ if $\zeta_n(z) < 0$. Then, we lower bound (3.51) by

$$\mathbb{D}(Q_{\alpha_n}\|Q_\emptyset) \overset{(a)}{\geqslant} \sum_z Q_\emptyset(z)\left(1+\frac{\alpha_n\zeta_n(z)}{Q_\emptyset(z)}\right)\left(\frac{\alpha_n\zeta_n(z)}{Q_\emptyset(z)} - \frac{\alpha_n^2\zeta_n^2(z)}{2Q_\emptyset^2(z)}\right)$$

$$+ \sum_{z:\zeta_n(z)<0} Q_\emptyset(z)\left(1+\frac{\alpha_n\zeta_n(z)}{Q_\emptyset(z)}\right)\left(\frac{2\alpha_n^3\zeta_n^3(z)}{3Q_\emptyset^3(z)}\right) \tag{3.54}$$

$$\overset{(b)}{\geqslant} \sum_z \frac{\alpha_n^2}{2}\left(\frac{\zeta_n^2(z)}{Q_\emptyset(z)} - \frac{\alpha_n\zeta_n^3(z)}{Q_\emptyset^2(z)}\right) + \sum_{z:\zeta_n(z)<0}\frac{2\alpha_n^3\zeta_n^3(z)}{3Q_\emptyset^2(z)}, \tag{3.55}$$

where, (a) follows from the inequalities $\log(1+x) > x - \frac{x^2}{2}$ for $x \geqslant 0$ and $\log(1+x) > x - \frac{x^2}{2} + \frac{2x^3}{3}$ for $x \in \left[-\frac{1}{2}, 0\right]$, and (b) follows from the fact that $\sum_z \zeta_n(z) = 0$. For n large enough, we loosen the bounds in (3.53) and (3.55) to obtain

$$\frac{\alpha_n^2}{2}\left(1+\sqrt{\alpha_n}\right)\chi_n(\boldsymbol{\rho}) \geqslant \mathbb{D}(Q_{\alpha_n}\|Q_\emptyset) \geqslant \frac{\alpha_n^2}{2}\left(1-\sqrt{\alpha_n}\right)\chi_n(\boldsymbol{\rho}). \tag{3.56}$$

From the definition of Q_{α_n}, we have

$$Q_{\alpha_n}(z) = Q_{\emptyset}(z) + \alpha_n \left(\sum_{k \in \mathcal{K}} \rho_k \left(Q_k(z) - Q_{\emptyset}(z) \right) \right) + \mathcal{O}\left(\alpha_n^2\right). \tag{3.57}$$

Using the definition of ζ_n and applying the limit, we obtain

$$\begin{aligned}
\lim_{n\to\infty} \zeta_n(z) &= \lim_{n\to\infty} \frac{Q_{\alpha_n}(z) - Q_{\emptyset}(z)}{\alpha_n} && (3.58)\\
&= \lim_{n\to\infty} \left(\sum_{k \in \mathcal{K}} \rho_k \left(Q_k(z) - Q_{\emptyset}(z) \right) + \mathcal{O}\left(\alpha_n\right) \right) && (3.59)\\
&\overset{(a)}{=} \sum_{k \in \mathcal{K}} \rho_k \left(Q_k(z) - Q_{\emptyset}(z) \right) && (3.60)\\
&= \zeta(z), && (3.61)
\end{aligned}$$

where (a) follows from the fact that $\lim_{n\to\infty} \alpha_n = 0$. From (3.61) and the definition of $\chi_n(\boldsymbol{\rho})$, it follows that

$$\lim_{n\to\infty} \chi_n(\boldsymbol{\rho}) = \lim_{n\to\infty} \sum_z \frac{\zeta_n^2(z)}{Q_{\emptyset}(z)} = \sum_z \frac{\zeta^2(z)}{Q_{\emptyset}(z)} = \chi(\boldsymbol{\rho}). \tag{3.62}$$

Finally, for a non-empty set $\mathcal{T} \subseteq \mathcal{K}$, define $\lambda_{n,\mathcal{T}}(z) \triangleq \frac{W_{Z|X[\mathcal{T}]}(z|x_\emptyset[\mathcal{T}]) - Q_\emptyset(z)}{\alpha_n}$. Note that $\sum_z \lambda_{n,\mathcal{T}}(z) = 0$. Then, for any non-empty set $\mathcal{T} \subseteq \mathcal{K}$, we have

$$\mathbb{I}(X[\mathcal{T}]; Z)$$

$$= \sum_{x[\mathcal{T}]} \sum_z \left(\prod_{k \in \mathcal{T}} \Pi_{X_k}(x_k) \right) W_{Z|X[\mathcal{T}]}(z|x[\mathcal{T}]) \log \left(\frac{W_{Z|X[\mathcal{T}]}(z|x[\mathcal{T}])}{Q_{\alpha_n}(z)} \right) \tag{3.63}$$

$$= \sum_{x[\mathcal{T}]} \sum_z \left(\prod_{k \in \mathcal{T}} \Pi_{X_k}(x_k) \right) W_{Z|X[\mathcal{T}]}(z|x[\mathcal{T}]) \log \left(\frac{W_{Z|X[\mathcal{T}]}(z|x[\mathcal{T}])}{Q_\emptyset(z)} \right) - \mathbb{D}(Q_{\alpha_n} \| Q_\emptyset) \tag{3.64}$$

$$\begin{aligned} &\overset{(a)}{=} \sum_{\substack{\mathcal{U} \subseteq \mathcal{T}: \\ |\mathcal{U}|>1}} \left(\prod_{k \in \mathcal{U}} \rho_k \alpha_n \right) \left(\prod_{k \in \mathcal{U}^c} (1 - \rho_k \alpha_n) \right) \sum_z W_{Z|X[\mathcal{T}]}(z|x_{\mathcal{U}}[\mathcal{T}]) \log \left(\frac{W_{Z|X[\mathcal{T}]}(z|x_{\mathcal{U}}[\mathcal{T}])}{Q_\emptyset(z)} \right) \\ &\quad + \sum_{k \in \mathcal{T}} \rho_k \alpha_n \left(\prod_{\substack{i \in \mathcal{T}: \\ i \neq k}} (1 - \rho_i \alpha_n) \right) \sum_z W_{Z|X[\mathcal{T}]}\left(z|x_{\{k\}}[\mathcal{T}]\right) \log \left(\frac{W_{Z|X[\mathcal{T}]}\left(z|x_{\{k\}}[\mathcal{T}]\right)}{Q_\emptyset(z)} \right) \\ &\quad + \left(\prod_{k \in \mathcal{T}} (1 - \rho_k \alpha_n) \right) \sum_z W_{Z|X[\mathcal{T}]}(z|x_\emptyset[\mathcal{T}]) \log \left(\frac{W_{Z|X[\mathcal{T}]}(z|x_\emptyset[\mathcal{T}])}{Q_\emptyset(z)} \right) - \mathbb{D}(Q_{\alpha_n} \| Q_\emptyset) \end{aligned} \tag{3.65}$$

$$= \sum_{k\in\mathcal{T}} \rho_k \alpha_n \left(\prod_{\substack{i\in\mathcal{T}:\\ i\neq k}} (1-\rho_i\alpha_n) \right) \sum_z W_{Z|X[\mathcal{T}]}\left(z|x_{\{k\}}[\mathcal{T}]\right) \log\left(\frac{W_{Z|X[\mathcal{T}]}\left(z|x_{\{k\}}[\mathcal{T}]\right)}{Q_\emptyset(z)} \right)$$

$$+ \left(\prod_{k\in\mathcal{T}} (1-\rho_k\alpha_n) \right) \sum_z \left(Q_\emptyset(z) + \alpha_n \lambda_{n,\mathcal{T}}(z)\right) \log\left(1+\alpha_n \frac{\lambda_{n,\mathcal{T}}(z)}{Q_\emptyset(z)}\right)$$

$$- \mathbb{D}(Q_{\alpha_n}\|Q_\emptyset) + \mathcal{O}\left(\alpha_n^2\right) \tag{3.66}$$

$$\overset{(b)}{=} \sum_{k\in\mathcal{T}} \rho_k\alpha_n \sum_z W_{Z|X[\mathcal{T}]}\left(z|x_{\{k\}}[\mathcal{T}]\right) \log\left(\frac{W_{Z|X[\mathcal{T}]}\left(z|x_{\{k\}}[\mathcal{T}]\right)}{Q_\emptyset(z)} \right) - \mathbb{D}(Q_{\alpha_n}\|Q_\emptyset) + \mathcal{O}\left(\alpha_n^2\right) \tag{3.67}$$

$$= \sum_{k\in\mathcal{T}} \rho_k\alpha_n \sum_z \left(Q_k(z) + \mathcal{O}\left(\alpha_n\right)\right) \log\left(\frac{Q_k(z)+\mathcal{O}\left(\alpha_n\right)}{Q_\emptyset(z)} \right) - \mathbb{D}(Q_{\alpha_n}\|Q_\emptyset) + \mathcal{O}\left(\alpha_n^2\right) \tag{3.68}$$

$$= \sum_{k\in\mathcal{T}} \rho_k\alpha_n \sum_z Q_k(z) \log\left(\left(\frac{Q_k(z)}{Q_\emptyset(z)} \right) \left(1 + \frac{\mathcal{O}\left(\alpha_n\right)}{Q_k(z)} \right) \right) - \mathbb{D}(Q_{\alpha_n}\|Q_\emptyset) + \mathcal{O}\left(\alpha_n^2\right) \tag{3.69}$$

$$= \sum_{k\in\mathcal{T}} \rho_k\alpha_n \left(\mathbb{D}(Q_k\|Q_\emptyset) + \sum_z Q_k(z) \log\left(1 + \frac{\mathcal{O}\left(\alpha_n\right)}{Q_k(z)} \right) \right) - \mathbb{D}(Q_{\alpha_n}\|Q_\emptyset) + \mathcal{O}\left(\alpha_n^2\right) \tag{3.70}$$

$$= \sum_{k\in\mathcal{T}} \rho_k\alpha_n \mathbb{D}(Q_k\|Q_\emptyset) - \mathbb{D}(Q_{\alpha_n}\|Q_\emptyset) + \mathcal{O}\left(\alpha_n^2\right), \tag{3.71}$$

where (a) follows from splitting the first term in (3.64) into three based on the number of users sending symbol 1, and (b) follows from the fact that the second term in (3.66) can be reduced to $\mathcal{O}\left(\alpha_n^2\right)$ by expanding $\log\left(1+\alpha_n\frac{\lambda_{n,\mathcal{T}}(z)}{Q_\emptyset(z)}\right)$ using Taylor series.

3.C Bernstein's inequality

Lemma 7. *Let $\{U_i\}_{i=1}^n$ be independent zero-mean random variables such that $|U_i| \leqslant c$ for a finite $c > 0$ almost surely for all $i \in [\![1, n]\!]$. Then, for any $t > 0$,*

$$\mathbb{P}\left(\sum_{i=1}^{n} U_i > t\right) \leqslant \exp\left(-\frac{\frac{1}{2}t^2}{\sum_{i=1}^{n}\mathbb{E}\left(U_i^2\right) + \frac{1}{3}ct}\right). \tag{3.72}$$

3.D Proof of Lemma 3

The K users encode messages $W[\mathcal{K}] = m[\mathcal{K}]$ using keys $S[\mathcal{K}] = \ell[\mathcal{K}]$ into codewords $\mathbf{x}_{\mathcal{K}}\left(m[\mathcal{K}], \ell[\mathcal{K}]\right)$ and transmit them over a discrete memoryless MAC. The following two events lead to a decoding error.

- The transmitted codewords do not satisfy $\left(\mathbf{x}_{\mathcal{K}}\left(m[\mathcal{K}], \ell[\mathcal{K}]\right), \mathbf{y}\right) \in \mathcal{A}_\gamma^n$.
- A different message vector $\widetilde{m}[\mathcal{K}] \neq m[\mathcal{K}]$ exists such that $\left(\mathbf{x}_{\mathcal{K}}\left(\widetilde{m}[\mathcal{K}], \ell[\mathcal{K}]\right), \mathbf{y}\right) \in \mathcal{A}_\gamma^n$.

Define the event

$$\mathcal{E}_{m[\mathcal{K}]} \triangleq \left\{\left(\mathbf{X}_{\mathcal{K}}\left(m[\mathcal{K}], \ell[\mathcal{K}]\right), \mathbf{Y}\right) \in \mathcal{A}_\gamma^n\right\}. \tag{3.73}$$

The probability of decoding error at the legitimate receiver averaged over all random codebooks is given by

$$\mathbb{E}\left(P_e^n\right) = \mathbb{P}\Big(\widehat{W}[\mathcal{K}] \neq W[\mathcal{K}]\Big) \tag{3.74}$$

$$= \mathbb{E}\left(\frac{1}{\left(\prod_{k\in\mathcal{K}} M_k\right)} \sum_{m[\mathcal{K}]} \sum_{\mathbf{y}} W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{y}|\mathbf{X}_{\mathcal{K}}\left(m[\mathcal{K}], \ell[\mathcal{K}]\right)\right) \times \mathbb{1}\left\{\mathcal{E}_{m[\mathcal{K}]}^c \cup \bigcup_{\widetilde{m}[\mathcal{K}]\neq m[\mathcal{K}]} \mathcal{E}_{\widetilde{m}[\mathcal{K}]}\right\}\right) \tag{3.75}$$

$$\overset{(a)}{\leqslant} \mathbb{E}\left(\frac{1}{\left(\prod_{k\in\mathcal{K}} M_k\right)} \sum_{m[\mathcal{K}]} \sum_{\mathbf{y}} W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{y}|\mathbf{X}_{\mathcal{K}}\left(m[\mathcal{K}], \ell[\mathcal{K}]\right)\right) \mathbb{1}\left\{\mathcal{E}_{m[\mathcal{K}]}^{c}\right\}\right)$$
$$+ \mathbb{E}\left(\frac{1}{\left(\prod_{k\in\mathcal{K}} M_k\right)} \sum_{m[\mathcal{K}]} \sum_{\mathbf{y}} W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{y}|\mathbf{X}_{\mathcal{K}}\left(m[\mathcal{K}], \ell[\mathcal{K}]\right)\right) \sum_{\widetilde{m}[\mathcal{K}]\neq m[\mathcal{K}]} \mathbb{1}\left\{\mathcal{E}_{\widetilde{m}[\mathcal{K}]}\right\}\right), \tag{3.76}$$

where (a) follows from the application of the union bound. We bound the first term in (3.76) by

$$\mathbb{E}\left(\frac{1}{\left(\prod_{k\in\mathcal{K}} M_k\right)} \sum_{m[\mathcal{K}]} \sum_{\mathbf{y}} W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{y}|\mathbf{X}_{\mathcal{K}}\left(m[\mathcal{K}], \ell[\mathcal{K}]\right)\right) \mathbb{1}\left\{\mathcal{E}_{m[\mathcal{K}]}^{c}\right\}\right)$$
$$= \sum_{\mathbf{x}[\mathcal{K}]} \sum_{\mathbf{y}} W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{y}|\mathbf{x}[\mathcal{K}]\right)\left(\prod_{k\in\mathcal{K}} \Pi_{X_k}^{\otimes n}\left(\mathbf{x}_k\right)\right) \mathbb{1}\left\{\left(\mathbf{x}[\mathcal{K}], \mathbf{y}\right) \in \mathcal{A}_{\gamma}^{nc}\right\} \tag{3.77}$$
$$= \mathbb{P}_{W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\prod_{k\in\mathcal{K}} \Pi_{X_k}^{\otimes n}\right)}\left(\mathcal{A}_{\gamma}^{nc}\right) \tag{3.78}$$
$$\overset{(a)}{\leqslant} \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \mathbb{P}_{W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\prod_{k\in\mathcal{K}} \Pi_{X_k}^{\otimes n}\right)}\left(\mathcal{A}_{\gamma_{\mathcal{T}}}^{n\ c}\right) \tag{3.79}$$
$$= \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \mathbb{P}_{W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\prod_{k\in\mathcal{K}} \Pi_{X_k}^{\otimes n}\right)}\left(\log \frac{W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{Y}|\mathbf{X}[\mathcal{K}]\right)}{W_{Y|X[\mathcal{T}^c]}^{\otimes n}\left(\mathbf{Y}|\mathbf{X}[\mathcal{T}^c]\right)} < \gamma_{\mathcal{T}}\right) \tag{3.80}$$
$$= \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \mathbb{P}_{W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\prod_{k\in\mathcal{K}} \Pi_{X_k}^{\otimes n}\right)}\left(\sum_{i=1}^{n} \log \frac{W_{Y|X[\mathcal{K}]}\left(Y|X[\mathcal{K}]\right)}{W_{Y|X[\mathcal{T}^c]}\left(Y|X[\mathcal{T}^c]\right)} < \gamma_{\mathcal{T}}\right), \tag{3.81}$$

where (a) follows from the fact that $\mathcal{A}_{\gamma}^{nc} = \bigcup_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \mathcal{A}_{\gamma_{\mathcal{T}}}^{n\ c}$ and the union bound. Define a zero-mean[5] random variable $U_{\mathcal{T}} \triangleq \mathbb{I}(X[\mathcal{T}]; Y|X[\mathcal{T}^c]) - \log \frac{W_{Y|X[\mathcal{K}]}(Y|X[\mathcal{K}])}{W_{Y|X[\mathcal{T}^c]}(Y|X[\mathcal{T}^c])}$. Note that $|U_{\mathcal{T}}|$ is bounded almost surely, and

$$\mathbb{E}\left(U_{\mathcal{T}}^2\right) = \mathbb{E}\left(\log^2 \frac{W_{Y|X[\mathcal{K}]}\left(Y|X[\mathcal{K}]\right)}{W_{Y|X[\mathcal{T}^c]}\left(Y|X[\mathcal{T}^c]\right)}\right) - \left(\mathbb{I}\left(X[\mathcal{T}]; Y|X[\mathcal{T}^c]\right)\right)^2. \tag{3.82}$$

[5]since $\mathbb{E}\left(\log \frac{W_{Y|X[\mathcal{K}]}(Y|X[\mathcal{K}])}{W_{Y|X[\mathcal{T}^c]}(Y|X[\mathcal{T}^c])}\right) = \mathbb{I}(X[\mathcal{T}]; Y|X[\mathcal{T}^c])$.

Let us analyze the expectation term on the right hand side of (3.82).

$$\begin{aligned}
&\mathbb{E}\left(\log^2 \frac{W_{Y|X[\mathcal{K}]}\left(Y|X[\mathcal{K}]\right)}{W_{Y|X[\mathcal{T}^c]}\left(Y|X[\mathcal{T}^c]\right)}\right) \\
&\quad = \sum_y \sum_{x[\mathcal{K}]} \left(\prod_{k\in\mathcal{K}} \Pi_{X_k}\left(x_k\right)\right) W_{Y|X[\mathcal{K}]}\left(y|x[\mathcal{K}]\right) \log^2 \frac{W_{Y|X[\mathcal{K}]}\left(y|x[\mathcal{K}]\right)}{W_{Y|X[\mathcal{T}^c]}\left(y|x[\mathcal{T}^c]\right)} \qquad (3.83) \\
&\quad \overset{(a)}{=} \sum_y \sum_{x[\mathcal{K}]\neq x_\emptyset[\mathcal{K}]} \left(\prod_{k\in\mathcal{K}} \Pi_{X_k}\left(x_k\right)\right) W_{Y|X[\mathcal{K}]}\left(y|x[\mathcal{K}]\right) \log^2 \frac{W_{Y|X[\mathcal{K}]}\left(y|x[\mathcal{K}]\right)}{W_{Y|X[\mathcal{T}^c]}\left(y|x[\mathcal{T}^c]\right)} \\
&\qquad + \sum_y \left(\prod_{k\in\mathcal{K}} \left(1-\rho_k\alpha_n\right)\right) P_\emptyset(y) \log^2 \frac{P_\emptyset(y)}{W_{Y|X[\mathcal{T}^c]}\left(y|x_\emptyset[\mathcal{T}^c]\right)} \qquad (3.84) \\
&\quad \overset{(b)}{=} \sum_y \left(\prod_{k\in\mathcal{K}} \left(1-\rho_k\alpha_n\right)\right) P_\emptyset(y) \log^2 \frac{P_\emptyset(y)}{W_{Y|X[\mathcal{T}^c]}\left(y|x_\emptyset[\mathcal{T}^c]\right)} + \mathcal{O}\left(\alpha_n\right) \qquad (3.85) \\
&\quad \overset{(c)}{=} \sum_y P_\emptyset(y) \log^2 \frac{W_{Y|X[\mathcal{T}^c]}\left(y|x_\emptyset[\mathcal{T}^c]\right)}{P_\emptyset(y)} + \mathcal{O}\left(\alpha_n\right), \qquad (3.86)
\end{aligned}$$

where (a) follows from splitting the first sum on the right hand side of (3.83) into two based on whether $x\left[\mathcal{K}\right]$ equals $x_\emptyset\left[\mathcal{K}\right]$ or not, (b) follows from the fact that the first term in (3.84) is on the order of α_n since at least one of the symbols in $x\left[\mathcal{K}\right]$ is a 1, and (c) follows from the expansion of the product term and the fact that $\log^2 \frac{P_\emptyset(y)}{W_{Y|X[\mathcal{T}^c]}(y|x_\emptyset[\mathcal{T}^c])} = \log^2 \frac{W_{Y|X[\mathcal{T}^c]}(y|x_\emptyset[\mathcal{T}^c])}{P_\emptyset(y)}$. Expanding the numerator in the $\log^2$ term in (3.86), we obtain

$$\begin{aligned}
W_{Y|X[\mathcal{T}^c]}\left(y|x_\emptyset[\mathcal{T}^c]\right) &= \sum_{x[\mathcal{T}]} \left(\prod_{k\in\mathcal{T}} \Pi_{X_k}\left(x\left[\{k\}\right]\right)\right) W_{Y|X[\mathcal{T}^c]X[\mathcal{T}]}\left(y|x_\emptyset\left[\mathcal{T}^c\right]x\left[\mathcal{T}\right]\right) \qquad (3.87) \\
&= \sum_{x[\mathcal{T}]\neq x_\emptyset[\mathcal{T}]} \left(\prod_{k\in\mathcal{T}} \Pi_{X_k}\left(x\left[\{k\}\right]\right)\right) W_{Y|X[\mathcal{T}^c]X[\mathcal{T}]}\left(y|x_\emptyset\left[\mathcal{T}^c\right]x\left[\mathcal{T}\right]\right) \\
&\qquad + \left(\prod_{k\in\mathcal{T}} \left(1-\rho_k\alpha_n\right)\right) P_\emptyset(y) \qquad (3.88) \\
&\overset{(a)}{=} P_\emptyset(y) + \mathcal{O}\left(\alpha_n\right), \qquad (3.89)
\end{aligned}$$

where (a) follows from the fact that the first term in (3.88) is on the order of α_n since at least one of the symbols in $x\left[\mathcal{T}\right]$ is a 1 and from the expansion of the product term. Combining (3.86) and (3.89), we obtain

$$\mathbb{E}\left(\log^2 \frac{W_{Y|X[\mathcal{K}]}\left(Y|X[\mathcal{K}]\right)}{W_{Y|X[\mathcal{T}^c]}\left(Y|X[\mathcal{T}^c]\right)}\right) = \sum_y P_\emptyset(y) \log^2\left(1 + \frac{\mathcal{O}\left(\alpha_n\right)}{P_\emptyset(y)}\right) + \mathcal{O}\left(\alpha_n\right) \tag{3.90}$$

$$\stackrel{(a)}{=} \mathcal{O}\left(\alpha_n\right), \tag{3.91}$$

where (a) follows from using the Taylor series of the log term. Let us now analyze the mutual information term on the right hand side of (3.82).

$$\mathbb{I}\left(X[\mathcal{T}]; Y|X[\mathcal{T}^c]\right) = \mathbb{I}(X[\mathcal{K}]; Y) - \mathbb{I}(X[\mathcal{T}^c]; Y) \tag{3.92}$$

$$\stackrel{(a)}{=} \sum_{k\in\mathcal{K}} \rho_k \alpha_n \mathbb{D}(P_k \| P_\emptyset) - \sum_{k\in\mathcal{T}^c} \rho_k \alpha_n \mathbb{D}(P_k \| P_\emptyset) + \mathcal{O}\left(\alpha_n^2\right) \tag{3.93}$$

$$= \sum_{k\in\mathcal{T}} \rho_k \alpha_n \mathbb{D}(P_k \| P_\emptyset) + \mathcal{O}\left(\alpha_n^2\right), \tag{3.94}$$

where (a) follows from Lemma 2. Using the definition of $\gamma_{\mathcal{T}}$, for an arbitrary $\mu \in (0,1)$, we upper bound (3.81) using Bernstein's inequality as follows.

$$\mathbb{E}\left(\frac{1}{\left(\prod_{k\in\mathcal{K}} M_k\right)} \sum_{m[\mathcal{K}]} \sum_{\mathbf{y}} W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{y}|\mathbf{X}_{\mathcal{K}}\left(m[\mathcal{K}], 1[\mathcal{K}]\right)\right) \mathbb{1}\left\{\mathcal{E}_{m[\mathcal{K}]}^{c}\right\}\right)$$

$$\leqslant \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \mathbb{P}_{W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\prod_{k\in\mathcal{K}} \Pi_{X_k}^{\otimes n}\right)}\left(\sum_{i=1}^{n} \log \frac{W_{Y|X[\mathcal{K}]}\left(Y|X[\mathcal{K}]\right)}{W_{Y|X[\mathcal{T}^c]}\left(Y|X[\mathcal{T}^c]\right)} < \gamma_{\mathcal{T}}\right) \tag{3.95}$$

$$= \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \mathbb{P}\left(\sum_{i=1}^{n} U_{\mathcal{T}} > \mu n \mathbb{I}(X[\mathcal{T}]; Y|X[\mathcal{T}^c])\right) \tag{3.96}$$

$$\overset{(a)}{\leqslant} \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \exp\left(-\frac{\frac{1}{2}\left(\mu n \mathbb{I}(X[\mathcal{T}]; Y|X[\mathcal{T}^c])\right)^2}{n\mathcal{O}\left(\alpha_n\right) + \frac{1}{3} c\mu n \mathbb{I}(X[\mathcal{T}]; Y|X[\mathcal{T}^c])}\right) \tag{3.97}$$

$$\leqslant \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \exp\left(-c_1 n\alpha_n\right) \tag{3.98}$$

$$\overset{(b)}{\leqslant} \exp\left(-c_2 n\alpha_n\right), \tag{3.99}$$

for appropriate constants $c, c_1, c_2 > 0$, where (a) follows from using Bernstein's inequality, and (b) follows from the fact that, for a finite K, there exist $2^K - 1$ non-empty subsets of $\mathcal{K}$. Denoting the $|\mathcal{T}|$-length vector $(1, 1, \ldots, 1)$ by $1[\mathcal{T}]$ for any non-empty

set $\mathcal{T} \subseteq \mathcal{K}$, we upper bound the second term in (3.76) by

$$\mathbb{E}\left(\frac{1}{\left(\prod_{k\in\mathcal{K}} M_k\right)} \sum_{m[\mathcal{K}]} \sum_{\mathbf{y}} W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{y}|\mathbf{X}_{\mathcal{K}}\left(m[\mathcal{K}], \ell[\mathcal{K}]\right)\right) \sum_{\widetilde{m}[\mathcal{K}]\neq m[\mathcal{K}]} \mathbb{1}\left\{\mathcal{E}_{\widetilde{m}[\mathcal{K}]}\right\}\right)$$

$$\overset{(a)}{=} \mathbb{E}\left(\frac{1}{\left(\prod_{k\in\mathcal{K}} M_k\right)} \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \sum_{m[\mathcal{T}]} \sum_{m[\mathcal{T}^c]} \sum_{\substack{\widetilde{m}[\mathcal{T}]:\\ \widetilde{m}_k\neq m_k, \forall k\in\mathcal{T}}} \sum_{\mathbf{y}} W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{y}|\mathbf{X}_{\mathcal{K}}\left(m[\mathcal{K}], \ell[\mathcal{K}]\right)\right) \times \mathbb{1}\left\{\mathcal{E}_{\widetilde{m}[\mathcal{T}]m[\mathcal{T}^c]}\right\}\right) \tag{3.100}$$

$$\overset{(b)}{=} \sum_{\mathbf{y}} \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \sum_{\substack{\widetilde{m}[\mathcal{T}]:\\ \widetilde{m}_k\neq 1, \forall k\in\mathcal{T}}} \sum_{\mathbf{x}_{\mathcal{K}}(1[\mathcal{K}], \ell[\mathcal{K}])} \sum_{\mathbf{x}_{\mathcal{T}}(\widetilde{m}[\mathcal{T}], \ell[\mathcal{T}])} W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{y}|\mathbf{x}_{\mathcal{K}}\left(1[\mathcal{K}], \ell[\mathcal{K}]\right)\right)$$
$$\times \left(\prod_{k\in\mathcal{K}} \Pi_{X_k}^{\otimes n}\left(\mathbf{x}_k\left(1, \ell_k\right)\right)\right) \left(\prod_{k\in\mathcal{T}} \Pi_{X_k}^{\otimes n}\left(\mathbf{x}_k\left(\widetilde{m}_k, \ell_k\right)\right)\right)$$
$$\times \mathbb{1}\left\{\left(\mathbf{x}_{\mathcal{T}}\left(\widetilde{m}[\mathcal{T}], \ell[\mathcal{T}]\right), \mathbf{x}_{\mathcal{T}^c}\left(1[\mathcal{T}^c], \ell[\mathcal{T}^c]\right), \mathbf{y}\right) \in \mathcal{A}_\gamma^n\right\} \tag{3.101}$$

$$= \sum_{\mathbf{y}} \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \sum_{\substack{\widetilde{m}[\mathcal{T}]:\\ \widetilde{m}_k\neq 1, \forall k\in\mathcal{T}}} \sum_{\mathbf{x}_{\mathcal{T}^c}(1[\mathcal{T}^c], \ell[\mathcal{T}^c])} \sum_{\mathbf{x}_{\mathcal{T}}(\widetilde{m}[\mathcal{T}], \ell[\mathcal{T}])} W_{Y|X[\mathcal{T}^c]}^{\otimes n}\left(\mathbf{y}|\mathbf{x}_{\mathcal{T}^c}\left(1[\mathcal{T}^c], \ell[\mathcal{T}^c]\right)\right)$$
$$\times \left(\prod_{k\in\mathcal{T}^c} \Pi_{X_k}^{\otimes n}\left(\mathbf{x}_k\left(1, \ell_k\right)\right)\right) \left(\prod_{k\in\mathcal{T}} \Pi_{X_k}^{\otimes n}\left(\mathbf{x}_k\left(\widetilde{m}_k, \ell_k\right)\right)\right)$$
$$\times \mathbb{1}\left\{\left(\mathbf{x}_{\mathcal{T}}\left(\widetilde{m}[\mathcal{T}], \ell[\mathcal{T}]\right), \mathbf{x}_{\mathcal{T}^c}\left(1[\mathcal{T}^c], \ell[\mathcal{T}^c]\right), \mathbf{y}\right) \in \mathcal{A}_\gamma^n\right\} \tag{3.102}$$

$$\overset{(c)}{\leqslant} \sum_{\mathbf{y}} \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \sum_{\substack{\widetilde{m}[\mathcal{T}]:\\ \widetilde{m}_k\neq 1, \forall k\in\mathcal{T}}} \sum_{\mathbf{x}_{\mathcal{T}^c}(1[\mathcal{T}^c], \ell[\mathcal{T}^c])\mathbf{x}_{\mathcal{T}}(\widetilde{m}[\mathcal{T}], \ell[\mathcal{T}])} \sum W_{Y|X[\mathcal{T}^c]}^{\otimes n}\left(\mathbf{y}|\mathbf{x}_{\mathcal{T}^c}\left(1[\mathcal{T}^c], \ell[\mathcal{T}^c]\right)\right)$$
$$\times \left(\prod_{k\in\mathcal{T}^c} \Pi_{X_k}^{\otimes n}\left(\mathbf{x}_k\left(1, \ell_k\right)\right)\right) \left(\prod_{k\in\mathcal{T}} \Pi_{X_k}^{\otimes n}\left(\mathbf{x}_k\left(\widetilde{m}_k, \ell_k\right)\right)\right)$$
$$\times \mathbb{1}\left\{\left(\mathbf{x}_{\mathcal{T}}\left(\widetilde{m}[\mathcal{T}], \ell[\mathcal{T}]\right), \mathbf{x}_{\mathcal{T}^c}\left(1[\mathcal{T}^c], \ell[\mathcal{T}^c]\right), \mathbf{y}\right) \in \mathcal{A}_{\gamma_{\mathcal{T}}}^n\right\} \tag{3.103}$$

$$\leqslant \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} e^{-\gamma_{\mathcal{T}}} \left(\prod_{k\in\mathcal{T}} M_k\right) \left(\sum_{\mathbf{y}} \sum_{\mathbf{x}[\mathcal{K}]} W_{Y|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{y}|\mathbf{x}[\mathcal{K}]\right) \left(\prod_{k\in\mathcal{K}} \Pi_{X_k}^{\otimes n}\left(\mathbf{x}_k\right)\right)\right) \tag{3.104}$$

$$= \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} e^{-\gamma_{\mathcal{T}}} \left(\prod_{k\in\mathcal{T}} M_k\right), \tag{3.105}$$

where (a) follows from rewriting the left hand side of (3.100) in terms of the positions in which the two vectors $m\left[\mathcal{K}\right]$ and $\widetilde{m}\left[\mathcal{K}\right]$ do not match, (b) follows from setting $m\left[\mathcal{K}\right] = 1\left[\mathcal{K}\right]$ without loss of generality, and (c) follows from the fact that $\mathcal{A}_{\gamma}^{n}$ in the indicator function of (3.102) is a subset of $\mathcal{A}_{\gamma_{\mathcal{T}}}^{n}$ in the indicator function of (3.103) by definition of $\mathcal{A}_{\gamma}^{n}$. Combining (3.99) and (3.105), we upper bound (3.76) by

$$\mathbb{E}\left(P_e^n\right) \leqslant \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} e^{-\gamma_{\mathcal{T}}} \left(\prod_{k\in\mathcal{T}} M_k\right) + \exp\left(-c_2 n\alpha_n\right). \tag{3.106}$$

Using the definition of $\gamma_{\mathcal{T}}$, (3.94) and (3.106), we conclude that for an arbitrary $\delta \in (0,1)$ and n large enough, if

$$\sum_{k\in\mathcal{T}} \log M_k = (1-\delta)(1-\mu)\, n\alpha_n \sum_{k\in\mathcal{T}} \rho_k \mathbb{D}(P_k\|P_{\emptyset}), \tag{3.107}$$

for every non-empty set $\mathcal{T} \subseteq \mathcal{K}$, then there exists a constant $\xi > 0$ such that

$$\mathbb{E}\left(P_e^n\right) \leqslant \exp\left(-\xi n\alpha_n\right). \tag{3.108}$$

If $\mathcal{T}$ is a singleton set $\{k\}$, where $k \in \mathcal{K}$, it follows from (3.107) that

$$\log M_k = (1-\delta)(1-\mu)\, \rho_k n\alpha_n \mathbb{D}(P_k\|P_{\emptyset}). \tag{3.109}$$

Observing (3.107) and (3.109), we conclude that (3.107) is automatically satisfied for every non-empty set $\mathcal{T} \subseteq \mathcal{K}$, if $\log M_k$ satisfies (3.109) for every $k \in \mathcal{K}$.

3.E Proof of Lemma 4

Define the set $\mathcal{B}_{\eta}^{n} \triangleq \bigcap_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \mathcal{B}_{\eta_{\mathcal{T}}}^{n}$ with

$$\mathcal{B}_{\eta_{\mathcal{T}}}^{n} \triangleq \left\{ (\mathbf{x}[\mathcal{T}], \mathbf{z}) \in \mathcal{X}^{n}[\mathcal{T}] \times \mathcal{Z}^{n} : \log \frac{W_{Z|X[\mathcal{T}]}^{\otimes n}\left(\mathbf{z}|\mathbf{x}[\mathcal{T}]\right)}{Q_{\alpha_n}^{\otimes n}\left(\mathbf{z}\right)} \leqslant \eta_{\mathcal{T}} \right\}, \tag{3.110}$$

where

$$\eta_{\mathcal{T}} \triangleq (1+\mu)\, n\mathbb{I}(X[\mathcal{T}]; Z), \tag{3.111}$$

for every non-empty set $\mathcal{T} \subseteq \mathcal{K}$ and an arbitrary $\mu > 0$. For every $(m[\mathcal{K}], \ell[\mathcal{K}]) \in \times_{k=1}^{K}[\![1, M_k]\!] \times \times_{k=1}^{K}[\![1, L_k]\!]$, $\mathbb{E}_{\sim(m[\mathcal{K}],\ell[\mathcal{K}])}$ denotes the expectation taken over all n-length sequences $\left\{\mathbf{X}_{\mathcal{K}}\left(\widetilde{m}[\mathcal{K}], \widetilde{\ell}[\mathcal{K}]\right)\right\}_{\substack{\left(\widetilde{m}[\mathcal{K}],\widetilde{\ell}[\mathcal{K}]\right)\in\left(\times_{k=1}^{K}[\![1,M_k]\!]\times\times_{k=1}^{K}[\![1,L_k]\!]\right):\\ \left(\widetilde{m}[\mathcal{K}],\widetilde{\ell}[\mathcal{K}]\right)\neq(m[\mathcal{K}],\ell[\mathcal{K}])}}$. Let us analyze the KL divergence between $\widehat{Q}^{n}$ and $Q_{\alpha_n}^{\otimes n}$ averaged over all random codebooks.

$$\begin{aligned}
&\mathbb{E}\left(\mathbb{D}\left(\widehat{Q}^{n} \| Q_{\alpha_n}^{\otimes n}\right)\right) \\
&= \mathbb{E}\left(\sum_{\mathbf{z}} \widehat{Q}^{n}\left(\mathbf{z}\right) \log \frac{\widehat{Q}^{n}\left(\mathbf{z}\right)}{Q_{\alpha_n}^{\otimes n}\left(\mathbf{z}\right)}\right) &(3.112)\\
&= \mathbb{E}\left(\sum_{\mathbf{z}} \frac{\sum\limits_{m[\mathcal{K}]}\sum\limits_{\ell[\mathcal{K}]} W_{Z|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{z}|\mathbf{X}_{\mathcal{K}}\left(m[\mathcal{K}], \ell[\mathcal{K}]\right)\right)}{\left(\prod\limits_{k\in\mathcal{K}} M_k L_k\right)}\right. \\
&\qquad \left. \times \log\left(\frac{\sum\limits_{\widetilde{m}[\mathcal{K}]}\sum\limits_{\widetilde{\ell}[\mathcal{K}]} W_{Z|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{z}|\mathbf{X}_{\mathcal{K}}\left(\widetilde{m}[\mathcal{K}], \widetilde{\ell}[\mathcal{K}]\right)\right)}{\left(\prod\limits_{k\in\mathcal{K}} M_k L_k\right) Q_{\alpha_n}^{\otimes n}\left(\mathbf{z}\right)}\right)\right) &(3.113)\\
&\overset{(a)}{\leqslant} \sum_{\mathbf{z}}\sum_{m[\mathcal{K}]}\sum_{\ell[\mathcal{K}]}\sum_{\mathbf{x}_{\mathcal{K}}(m[\mathcal{K}],\ell[\mathcal{K}])} \frac{W_{Z|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{z}|\mathbf{x}_{\mathcal{K}}\left(m[\mathcal{K}], \ell[\mathcal{K}]\right)\right)\left(\prod_{k\in\mathcal{K}} \Pi_{X_k}^{\otimes n}\left(\mathbf{x}_k\left(m_k, \ell_k\right)\right)\right)}{\left(\prod_{k\in\mathcal{K}} M_k L_k\right)} \\
&\qquad \times \log \mathbb{E}_{\sim(m[\mathcal{K}],\ell[\mathcal{K}])}\left(\frac{\sum_{\widetilde{m}[\mathcal{K}]}\sum_{\widetilde{\ell}[\mathcal{K}]} W_{Z|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{z}|\mathbf{X}_{\mathcal{K}}\left(\widetilde{m}[\mathcal{K}], \widetilde{\ell}[\mathcal{K}]\right)\right)}{\left(\prod_{k\in\mathcal{K}} M_k L_k\right) Q_{\alpha_n}^{\otimes n}\left(\mathbf{z}\right)}\right), &(3.114)
\end{aligned}$$

where (a) follows from Jensen's inequality. Let us analyze the log term in (3.114).

$$\log \mathbb{E}_{\sim(m[\mathcal{K}],\ell[\mathcal{K}])}\left(\frac{\sum_{\widetilde{m}[\mathcal{K}]}\sum_{\widetilde{\ell}[\mathcal{K}]} W_{Z|X[\mathcal{K}]}^{\otimes n}\left(\mathbf{z}|\mathbf{X}_{\mathcal{K}}\left(\widetilde{m}[\mathcal{K}],\widetilde{\ell}[\mathcal{K}]\right)\right)}{\left(\prod_{k\in\mathcal{K}} M_k L_k\right) Q_{\alpha_n}^{\otimes n}(\mathbf{z})}\right)$$

$$= \log\left(\frac{\begin{array}{r}\sum_{\mathcal{T}\subseteq\mathcal{K}}\sum_{\widetilde{m}[\mathcal{T}^c]:\widetilde{m}_k\neq m_k,\forall k\in\mathcal{T}^c}\sum_{\widetilde{\ell}[\mathcal{T}^c]:\widetilde{\ell}_k\neq\ell_k,\forall k\in\mathcal{T}^c}\sum_{\mathbf{x}_{\mathcal{T}^c}\left(\widetilde{m}[\mathcal{T}^c],\widetilde{\ell}[\mathcal{T}^c]\right)} \\ W_{Z|X[\mathcal{T}]X[\mathcal{T}^c]}\left(\mathbf{z}|\mathbf{x}_{\mathcal{T}}\left(m\left[\mathcal{T}\right],\ell\left[\mathcal{T}\right]\right)\mathbf{x}_{\mathcal{T}^c}\left(\widetilde{m}\left[\mathcal{T}^c\right],\widetilde{\ell}\left[\mathcal{T}^c\right]\right)\right) \\ \left(\prod_{k\in\mathcal{T}^c}\Pi_{X_k}^{\otimes n}\left(\mathbf{x}_k\left(\widetilde{m}_k,\widetilde{\ell}_k\right)\right)\right)\end{array}}{\left(\prod_{k\in\mathcal{K}} M_k L_k\right) Q_{\alpha_n}^{\otimes n}(\mathbf{z})}\right) \tag{3.115}$$

$$\overset{(a)}{=} \log\left(\begin{array}{l}\frac{\begin{array}{r}\sum_{\mathcal{T}\subseteq\mathcal{K}:\,\mathcal{T}\neq\emptyset}\sum_{\widetilde{m}[\mathcal{T}^c]:\widetilde{m}_k\neq m_k,\forall k\in\mathcal{T}^c}\sum_{\widetilde{\ell}[\mathcal{T}^c]:\widetilde{\ell}_k\neq\ell_k,\forall k\in\mathcal{T}^c}\sum_{\mathbf{x}_{\mathcal{T}^c}\left(\widetilde{m}[\mathcal{T}^c],\widetilde{\ell}[\mathcal{T}^c]\right)} \\ W_{Z|X[\mathcal{T}]X[\mathcal{T}^c]}\left(\mathbf{z}|\mathbf{x}_{\mathcal{T}}\left(m\left[\mathcal{T}\right],\ell\left[\mathcal{T}\right]\right)\mathbf{x}_{\mathcal{T}^c}\left(\widetilde{m}\left[\mathcal{T}^c\right],\widetilde{\ell}\left[\mathcal{T}^c\right]\right)\right) \\ \left(\prod_{k\in\mathcal{T}^c}\Pi_{X_k}^{\otimes n}\left(\mathbf{x}_k\left(\widetilde{m}_k,\widetilde{\ell}_k\right)\right)\right)\end{array}}{\left(\prod_{k\in\mathcal{K}} M_k L_k\right) Q_{\alpha_n}^{\otimes n}(\mathbf{z})} \\ \\ +\frac{\begin{array}{r}\sum_{\widetilde{m}[\mathcal{K}]:\widetilde{m}_k\neq m_k,\forall k\in\mathcal{K}}\sum_{\widetilde{\ell}[\mathcal{K}]:\widetilde{\ell}_k\neq\ell_k,\forall k\in\mathcal{K}}\sum_{\mathbf{x}_{\mathcal{K}}\left(\widetilde{m}[\mathcal{K}],\widetilde{\ell}[\mathcal{K}]\right)} \\ W_{Z|X[\mathcal{K}]}\left(\mathbf{z}|\mathbf{x}_{\mathcal{K}}\left(\widetilde{m}\left[\mathcal{K}\right],\widetilde{\ell}\left[\mathcal{K}\right]\right)\right)\left(\prod_{k\in\mathcal{K}}\Pi_{X_k}^{\otimes n}\left(\mathbf{x}_k\left(\widetilde{m}_k,\widetilde{\ell}_k\right)\right)\right)\end{array}}{\left(\prod_{k\in\mathcal{K}} M_k L_k\right) Q_{\alpha_n}^{\otimes n}(\mathbf{z})}\end{array}\right) \tag{3.116}$$

$$\overset{(b)}{=} \log\left(\sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}}\frac{W_{Z|X[\mathcal{T}]}^{\otimes n}\left(\mathbf{z}|\mathbf{x}_{\mathcal{T}}\left(m[\mathcal{T}],\ell[\mathcal{T}]\right)\right)}{\left(\prod_{k\in\mathcal{T}} M_k L_k\right) Q_{\alpha_n}^{\otimes n}(\mathbf{z})} + \frac{\sum_{\widetilde{m}[\mathcal{K}]:\widetilde{m}_k\neq m_k,\forall k\in\mathcal{K}}\sum_{\widetilde{\ell}[\mathcal{K}]:\widetilde{\ell}_k\neq\ell_k,\forall k\in\mathcal{K}} Q_{\alpha_n}^{\otimes n}(\mathbf{z})}{\left(\prod_{k\in\mathcal{K}} M_k L_k\right) Q_{\alpha_n}^{\otimes n}(\mathbf{z})}\right) \tag{3.117}$$

$$\leqslant \log\left(\sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}}\frac{W_{Z|X[\mathcal{T}]}^{\otimes n}\left(\mathbf{z}|\mathbf{x}_{\mathcal{T}}\left(m[\mathcal{T}],\ell[\mathcal{T}]\right)\right)}{\left(\prod_{k\in\mathcal{T}} M_k L_k\right) Q_{\alpha_n}^{\otimes n}(\mathbf{z})} + 1\right) \tag{3.118}$$

$$= \log\left(\sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \frac{W_{Z|X[\mathcal{T}]}^{\otimes n}\left(\mathbf{z}|\mathbf{x}_{\mathcal{T}}\left(m[\mathcal{T}],\ell[\mathcal{T}]\right)\right)}{\left(\prod_{k\in\mathcal{T}} M_k L_k\right) Q_{\alpha_n}^{\otimes n}(\mathbf{z})} + 1\right) \mathbb{1}\left\{\left(\mathbf{x}_{\mathcal{K}}\left(m[\mathcal{K}],\ell[\mathcal{K}]\right),\mathbf{z}\right)\in\mathcal{B}_\eta^n\right\}$$
$$+ \log\left(\sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \frac{W_{Z|X[\mathcal{T}]}^{\otimes n}\left(\mathbf{z}|\mathbf{x}_{\mathcal{T}}\left(m[\mathcal{T}],\ell[\mathcal{T}]\right)\right)}{\left(\prod_{k\in\mathcal{T}} M_k L_k\right) Q_{\alpha_n}^{\otimes n}(\mathbf{z})} + 1\right) \mathbb{1}\left\{\left(\mathbf{x}_{\mathcal{K}}\left(m[\mathcal{K}],\ell[\mathcal{K}]\right),\mathbf{z}\right)\notin\mathcal{B}_\eta^n\right\}, \tag{3.119}$$

where (a) follows from splitting the numerator term in (3.115) into two based on whether $\mathcal{T}$ is empty or not and (b) follows from the fact that

$$\sum_{\mathbf{x}_{\mathcal{K}}\left(\widetilde{m}[\mathcal{K}],\widetilde{\ell}[\mathcal{K}]\right)} W_{Z|X[\mathcal{K}]}\left(\mathbf{z}|\mathbf{x}_{\mathcal{K}}\left(\widetilde{m}\left[\mathcal{K}\right],\widetilde{\ell}\left[\mathcal{K}\right]\right)\right)\left(\prod_{k\in\mathcal{K}}\Pi_{X_k}^{\otimes n}\left(\mathbf{x}_k\left(\widetilde{m}_k,\widetilde{\ell}_k\right)\right)\right) = Q_{\alpha_n}^{\otimes n}(\mathbf{z}).\tag{3.120}$$

We upper bound the first term in (3.119) by

$$\log\left(\sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \frac{W_{Z|X[\mathcal{T}]}^{\otimes n}\left(\mathbf{z}|\mathbf{x}_{\mathcal{T}}\left(m[\mathcal{T}],\ell[\mathcal{T}]\right)\right)}{\left(\prod_{k\in\mathcal{T}} M_k L_k\right) Q_{\alpha_n}^{\otimes n}(\mathbf{z})} + 1\right) \mathbb{1}\left\{\left(\mathbf{x}_{\mathcal{K}}\left(m[\mathcal{K}],\ell[\mathcal{K}]\right),\mathbf{z}\right)\in\mathcal{B}_\eta^n\right\}$$
$$\leqslant \log\left(\sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \frac{e^{\eta\tau}}{\left(\prod_{k\in\mathcal{T}} M_k L_k\right)} + 1\right) \tag{3.121}$$
$$\leqslant \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \frac{e^{\eta\tau}}{\left(\prod_{k\in\mathcal{T}} M_k L_k\right)}. \tag{3.122}$$

Defining $\nu_{\min} \triangleq \min_z Q_\emptyset(z)$, we upper bound the second term in (3.119) by

$$\log\left(\sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \frac{W_{Z|X[\mathcal{T}]}^{\otimes n}\left(\mathbf{z}|\mathbf{x}_{\mathcal{T}}\left(m[\mathcal{T}],\ell[\mathcal{T}]\right)\right)}{\left(\prod_{k\in\mathcal{T}} M_k L_k\right) Q_{\alpha_n}^{\otimes n}\left(\mathbf{z}\right)} + 1\right) \mathbb{1}\left\{\left(\mathbf{x}_{\mathcal{K}}\left(m[\mathcal{K}],\ell[\mathcal{K}]\right),\mathbf{z}\right)\notin\mathcal{B}_\eta^n\right\}$$

$$\leqslant \left(\log\left(\frac{1}{Q_{\alpha_n}^{\otimes n}\left(\mathbf{z}\right)}\right) + \log\left(\sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \frac{W_{Z|X[\mathcal{T}]}^{\otimes n}\left(\mathbf{z}|\mathbf{x}_{\mathcal{T}}\left(m[\mathcal{T}],\ell[\mathcal{T}]\right)\right)}{\left(\prod_{k\in\mathcal{T}} M_k L_k\right)} + Q_{\alpha_n}^{\otimes n}(\mathbf{z})\right)\right)$$

$$\times\, \mathbb{1}\left\{\left(\mathbf{x}_{\mathcal{K}}\left(m[\mathcal{K}],\ell[\mathcal{K}]\right),\mathbf{z}\right)\notin\mathcal{B}_\eta^n\right\} \tag{3.123}$$

$$\overset{(a)}{\leqslant} \left(n\log\left(\frac{1}{\left(\prod_{k\in\mathcal{K}}\left(1-\rho_k\alpha_n\right)\right)\nu_{\min}}\right) + \log\left(\sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} 1 + 1\right)\right)$$

$$\times\, \mathbb{1}\left\{\left(\mathbf{x}_{\mathcal{K}}\left(m[\mathcal{K}],\ell[\mathcal{K}]\right),\mathbf{z}\right)\notin\mathcal{B}_\eta^n\right\} \tag{3.124}$$

$$\overset{(b)}{\leqslant} \left(n\log\left(\frac{1}{\left(\prod_{k\in\mathcal{K}}\left(1-\rho_k\alpha_n\right)\right)\nu_{\min}}\right) + \log\left(2^K\right)\right) \mathbb{1}\left\{\left(\mathbf{x}_{\mathcal{K}}\left(m[\mathcal{K}],\ell[\mathcal{K}]\right),\mathbf{z}\right)\notin\mathcal{B}_\eta^n\right\} \tag{3.125}$$

$$\leqslant n\log\left(\frac{2^K}{\left(\prod_{k\in\mathcal{K}}\left(1-\rho_k\alpha_n\right)\right)\nu_{\min}}\right) \mathbb{1}\left\{\left(\mathbf{x}_{\mathcal{K}}\left(m[\mathcal{K}],\ell[\mathcal{K}]\right),\mathbf{z}\right)\notin\mathcal{B}_\eta^n\right\}, \tag{3.126}$$

where (a) follows from the fact that we can upper bound both $\frac{W_{Z|X[\mathcal{T}]}^{\otimes n}\left(\mathbf{z}|\mathbf{x}_{\mathcal{T}}\left(m[\mathcal{T}],\ell[\mathcal{T}]\right)\right)}{\left(\prod_{k\in\mathcal{T}} M_k L_k\right)}$ and $Q_{\alpha_n}^{\otimes n}(\mathbf{z})$ by 1 and (b) follows from the fact that there only exist 2^K-1 non-empty subsets of $\mathcal{K}$. Combining (3.122) and (3.126), we upper bound (3.114) by

$$\mathbb{E}\left(\mathbb{D}\left(\widehat{Q}^n\|Q_{\alpha_n}^{\otimes n}\right)\right) \leqslant \sum_{\mathbf{z}} Q_{\alpha_n}^{\otimes n}\left(\mathbf{z}\right)\left(\sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \frac{e^{\eta\tau}}{\left(\prod_{k\in\mathcal{T}} M_k L_k\right)}\right)$$

$$+ n\log\left(\frac{2^K}{\prod_{k\in\mathcal{K}}\left(1-\rho_k\alpha_n\right)\nu_{\min}}\right)\mathbb{P}\left(\mathcal{B}_\eta^{nc}\right) \tag{3.127}$$

$$= \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \frac{e^{\eta\tau}}{\left(\prod_{k\in\mathcal{T}} M_k L_k\right)} + n\log\left(\frac{2^K}{\prod_{k\in\mathcal{K}}\left(1-\rho_k\alpha_n\right)\nu_{\min}}\right)\mathbb{P}\left(\mathcal{B}_\eta^{nc}\right). \tag{3.128}$$

From the definition of $\mathcal{B}_{\eta}^{n}$, we obtain

$$\mathbb{P}\big(\mathcal{B}_{\eta}^{n\,c}\big) \leqslant \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \mathbb{P}\big(\mathcal{B}_{\eta_{\mathcal{T}}}^{n\ c}\big), \tag{3.129}$$

which follows from the fact that $\mathcal{B}_{\eta}^{n\,c} = \bigcup_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \mathcal{B}_{\eta_{\mathcal{T}}}^{n\ c}$ and the application of the union bound. We define a zero-mean random variable $V_{\mathcal{T}} \triangleq \log \frac{W_{Z|X[\mathcal{T}]}(Z|X[\mathcal{T}])}{Q_{\alpha_n}(Z)} - \mathbb{I}(X[\mathcal{T}];Z)$ since $\mathbb{E}\left(\log \frac{W_{Z|X[\mathcal{T}]}(Z|X[\mathcal{T}])}{Q_{\alpha_n}(Z)}\right) = \mathbb{I}(X[\mathcal{T}];Z)$. Note that $|V_{\mathcal{T}}|$ is bounded almost surely, and

$$\mathbb{E}\left(V_{\mathcal{T}}^2\right) = \mathbb{E}\left(\log^2 \frac{W_{Z|X[\mathcal{T}]}(Z|X[\mathcal{T}])}{Q_{\alpha_n}(Z)}\right) - \left(\mathbb{I}(X\left[\mathcal{T}\right];Z)\right)^2 \tag{3.130}$$

$$\stackrel{(a)}{=} \mathbb{E}\left(\log^2 \frac{W_{Z|X[\mathcal{T}]}(Z|X[\mathcal{T}])}{Q_{\alpha_n}(Z)}\right) + \mathcal{O}\left(\alpha_n^2\right), \tag{3.131}$$

where (a) follows from Lemma 2. Let us analyze the expectation term in (3.131).

$$\mathbb{E}\left(\log^2 \frac{W_{Z|X[\mathcal{T}]}(Z|X[\mathcal{T}])}{Q_{\alpha_n}(Z)}\right)$$

$$= \sum_{z}\sum_{x[\mathcal{T}]}\left(\prod_{k\in\mathcal{T}}\Pi_{X_k}(x_k)\right) W_{Z|X[\mathcal{T}]}(z|x[\mathcal{T}]) \log^2 \frac{W_{Z|X[\mathcal{T}]}(z|x[\mathcal{T}])}{Q_{\alpha_n}(z)} \tag{3.132}$$

$$\stackrel{(a)}{=} \sum_{z}\left(\prod_{k\in\mathcal{T}}(1-\rho_k\alpha_n)\right) W_{Z|X[\mathcal{T}]}(z|x_{\emptyset}[\mathcal{T}]) \log^2 \frac{W_{Z|X[\mathcal{T}]}(z|x_{\emptyset}[\mathcal{T}])}{Q_{\alpha_n}(z)}$$

$$+ \sum_{z}\sum_{x[\mathcal{T}]\neq x_{\emptyset}[\mathcal{T}]}\left(\prod_{k\in\mathcal{T}}\Pi_{X_k}(x_k)\right) W_{Z|X[\mathcal{T}]}(z|x[\mathcal{T}]) \log^2 \frac{W_{Z|X[\mathcal{T}]}(z|x[\mathcal{T}])}{Q_{\alpha_n}(z)} \tag{3.133}$$

$$\stackrel{(b)}{=} \sum_{z}\left(\prod_{k\in\mathcal{T}}(1-\rho_k\alpha_n)\right) W_{Z|X[\mathcal{T}]}(z|x_{\emptyset}[\mathcal{T}]) \log^2 \frac{W_{Z|X[\mathcal{T}]}(z|x_{\emptyset}[\mathcal{T}])}{Q_{\alpha_n}(z)} + \mathcal{O}\left(\alpha_n\right)$$

$$\tag{3.134}$$

$$\stackrel{(c)}{=} \sum_{z} W_{Z|X[\mathcal{T}]}(z|x_{\emptyset}[\mathcal{T}]) \log^2 \frac{Q_{\alpha_n}(z)}{W_{Z|X[\mathcal{T}]}(z|x_{\emptyset}[\mathcal{T}])} + \mathcal{O}\left(\alpha_n\right), \tag{3.135}$$

where (a) follows from splitting the term on the right hand side of (3.132) into two based on whether $x\left[\mathcal{T}\right] = x_{\emptyset}\left[\mathcal{T}\right]$ or not, (b) follows from the fact that at least one of

the symbols in $x[\mathcal{T}]$ in the second term in (3.133) is the symbol 1, and (c) follows from the expansion of the product term. From the definition of Q_{α_n}, we obtain

$$Q_{\alpha_n}(z) = \sum_{x[\mathcal{T}]} W_{Z|X[\mathcal{T}]}(z|x[\mathcal{T}]) \left(\prod_{k\in\mathcal{T}} \Pi_{X_k}(x_k) \right) \tag{3.136}$$

$$= \sum_{x[\mathcal{T}]\neq x_\emptyset[\mathcal{T}]} W_{Z|X[\mathcal{T}]}(z|x[\mathcal{T}]) \left(\prod_{k\in\mathcal{T}} \Pi_{X_k}(x_k) \right) + W_{Z|X[\mathcal{T}]}(z|x_\emptyset[\mathcal{T}]) \left(\prod_{k\in\mathcal{T}} (1-\rho_k\alpha_n) \right) \tag{3.137}$$

$$= W_{Z|X[\mathcal{T}]}(z|x_\emptyset[\mathcal{T}]) + \mathcal{O}(\alpha_n). \tag{3.138}$$

Combining (3.135) and (3.138), we obtain

$$\mathbb{E}\left(\log^2 \frac{W_{Z|X[\mathcal{T}]}(Z|X[\mathcal{T}])}{Q_{\alpha_n}(Z)} \right) = \sum_z W_{Z|X[\mathcal{T}]}(z|x_\emptyset[\mathcal{T}]) \log^2 \left(1 + \frac{\mathcal{O}(\alpha_n)}{W_{Z|X[\mathcal{T}]}(z|x_\emptyset[\mathcal{T}])} \right) + \mathcal{O}(\alpha_n) \tag{3.139}$$

$$\overset{(a)}{=} \mathcal{O}(\alpha_n), \tag{3.140}$$

where (a) follows from the application of the Taylor series of the log term. Using the definition of $\eta_\mathcal{T}$ in (3.111), for an arbitrary $\mu > 0$, we upper bound (3.129) by

$$\mathbb{P}\left(\mathcal{B}_\eta^{nc}\right) \leqslant \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \mathbb{P}\left(\log \frac{W_{Z|X[\mathcal{T}]}^{\otimes n}(\mathbf{Z}|\mathbf{X}[\mathcal{T}])}{Q_{\alpha_n}^{\otimes n}(\mathbf{Z})} > \eta_\mathcal{T} \right) \tag{3.141}$$

$$= \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \mathbb{P}\left(\sum_{i=1}^n \log \frac{W_{Z|X[\mathcal{T}]}(Z|X[\mathcal{T}])}{Q_{\alpha_n}(Z)} > (1+\mu)\, n\mathbb{I}(X[\mathcal{T}];Z) \right) \tag{3.142}$$

$$= \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \mathbb{P}\left(\sum_{i=1}^n V_\mathcal{T} > \mu n\mathbb{I}(X[\mathcal{T}];Z) \right) \tag{3.143}$$

$$\overset{(a)}{\leqslant} \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \exp\left(-\frac{\frac{1}{2}\left(\mu n\mathbb{I}(X[\mathcal{T}];Z)\right)^2}{n\mathcal{O}(\alpha_n) + \frac{1}{3}c\mu n\mathbb{I}(X[\mathcal{T}];Z)} \right) \tag{3.144}$$

$$\overset{(b)}{\leqslant} \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \exp\left(-c_1 n\alpha_n\right) \tag{3.145}$$

$$\leqslant \exp\left(-c_2 n\alpha_n\right), \tag{3.146}$$

for appropriate constants $c, c_1, c_2 > 0$, where (a) follows from using Bernstein's inequality, and (b) follows from the fact that $\mathbb{I}\left(X[\mathcal{T}]; Z\right) = \sum_{k\in\mathcal{T}} \rho_k \alpha_n \mathbb{D}(Q_k \| Q_\emptyset) + \mathcal{O}\left(\alpha_n^2\right)$, for any non-empty set $\mathcal{T} \subseteq \mathcal{K}$, from Lemma 2. Combining (3.128) and (3.146), for an appropriate constant $c_3 > 0$, we obtain

$$\mathbb{E}\left(\mathbb{D}\Big(\widehat{Q}^n \| Q_{\alpha_n}^{\otimes n}\Big)\right) \leqslant \sum_{\substack{\mathcal{T}\subseteq\mathcal{K}:\\ \mathcal{T}\neq\emptyset}} \frac{e^{\eta_{\mathcal{T}}}}{\left(\prod_{k\in\mathcal{T}} M_k L_k\right)} + \exp\left(-c_3 n\alpha_n\right). \tag{3.147}$$

Using the definition of $\eta_{\mathcal{T}}$, we conclude from (3.147) that for an arbitrary $\delta \in (0,1)$ and a large n, if

$$\sum_{k\in\mathcal{T}} \log(M_k L_k) = (1+\delta)(1+\mu)\, n\alpha_n \sum_{k\in\mathcal{T}} \rho_k \mathbb{D}(Q_k \| Q_\emptyset), \tag{3.148}$$

for every non-empty set $\mathcal{T} \subseteq \mathcal{K}$, then there exists a constant $\xi > 0$, such that

$$\mathbb{E}\left(\mathbb{D}\Big(\widehat{Q}^n \| Q_{\alpha_n}^{\otimes n}\Big)\right) \leqslant \exp\left(-\xi n\alpha_n\right). \tag{3.149}$$

If $\mathcal{T}$ is a singleton set $\{k\}$, where $k \in \mathcal{K}$, it follows from (3.148) that

$$\log(M_k L_k) = (1+\delta)(1+\mu)\, \rho_k n\alpha_n \mathbb{D}(Q_k \| Q_\emptyset). \tag{3.150}$$

Observing (3.148) and (3.150), we conclude that (3.148) is automatically satisfied for every non-empty set $\mathcal{T} \subseteq \mathcal{K}$, if $\log M_k L_k$ satisfies (3.150) for every $k \in \mathcal{K}$.

3.F Proof of Lemma 5

Since $\mathbb{D}\Big(\widehat{Q}^n \| Q_{\alpha_n}^{\otimes n}\Big) \leqslant \exp\left(-\xi_2 n\alpha_n\right)$, from Pinsker's inequality, we have $\mathbb{V}\Big(\widehat{Q}^n, Q_{\alpha_n}^{\otimes n}\Big) \leqslant \exp\left(-\frac{1}{2}\xi_2 n\alpha_n\right)$. Furthermore, we write

$$\mathbb{D}\Big(\widehat{Q}^n \| Q_{\emptyset}^{\otimes n}\Big) = \mathbb{D}\Big(\widehat{Q}^n \| Q_{\alpha_n}^{\otimes n}\Big) + \sum_{\mathbf{z}} \widehat{Q}^n(\mathbf{z}) \log\left(\frac{Q_{\alpha_n}^{\otimes n}(\mathbf{z})}{Q_{\emptyset}^{\otimes n}(\mathbf{z})}\right) \tag{3.151}$$

$$= \mathbb{D}\Big(\widehat{Q}^n \| Q_{\alpha_n}^{\otimes n}\Big) + \mathbb{D}\big(Q_{\alpha_n}^{\otimes n} \| Q_{\emptyset}^{\otimes n}\big) + \sum_{\mathbf{z}} \Big(\widehat{Q}^n(\mathbf{z}) - Q_{\alpha_n}^{\otimes n}(\mathbf{z})\Big) \log\left(\frac{Q_{\alpha_n}^{\otimes n}(\mathbf{z})}{Q_{\emptyset}^{\otimes n}(\mathbf{z})}\right). \tag{3.152}$$

Rearranging the terms in (3.152) and taking the absolute value yields

$$\left|\mathbb{D}\Big(\widehat{Q}^n \| Q_{\emptyset}^{\otimes n}\Big) - \mathbb{D}\big(Q_{\alpha_n}^{\otimes n} \| Q_{\emptyset}^{\otimes n}\big)\right| \leqslant \mathbb{D}\Big(\widehat{Q}^n \| Q_{\alpha_n}^{\otimes n}\Big) + \left|\sum_{\mathbf{z}} \Big(\widehat{Q}^n(\mathbf{z}) - Q_{\alpha_n}^{\otimes n}(\mathbf{z})\Big) \log\left(\frac{Q_{\alpha_n}^{\otimes n}(\mathbf{z})}{Q_{\emptyset}^{\otimes n}(\mathbf{z})}\right)\right|. \tag{3.153}$$

Defining $\nu_{\min} \triangleq \min_z Q_{\emptyset}(z)$, we bound the second term on the right hand side of (3.153) for n large enough as follows.

$$\left|\sum_{\mathbf{z}} \Big(\widehat{Q}^n(\mathbf{z}) - Q_{\alpha_n}^{\otimes n}(\mathbf{z})\Big) \log\left(\frac{Q_{\alpha_n}^{\otimes n}(\mathbf{z})}{Q_{\emptyset}^{\otimes n}(\mathbf{z})}\right)\right|$$

$$\leqslant \sum_{\mathbf{z}} \left|\widehat{Q}^n(\mathbf{z}) - Q_{\alpha_n}^{\otimes n}(\mathbf{z})\right| \left|\log\left(\frac{Q_{\alpha_n}^{\otimes n}(\mathbf{z})}{Q_{\emptyset}^{\otimes n}(\mathbf{z})}\right)\right| \tag{3.154}$$

$$= \sum_{\mathbf{z}} \left|\widehat{Q}^n(\mathbf{z}) - Q_{\alpha_n}^{\otimes n}(\mathbf{z})\right| \left(\log\left(\frac{Q_{\alpha_n}^{\otimes n}(\mathbf{z})}{Q_{\emptyset}^{\otimes n}(\mathbf{z})}\right) \mathbb{1}\left\{Q_{\alpha_n}^{\otimes n}(\mathbf{z}) \geqslant Q_{\emptyset}^{\otimes n}(\mathbf{z})\right\}\right.$$

$$\left. + \log\left(\frac{Q_{\emptyset}^{\otimes n}(\mathbf{z})}{Q_{\alpha_n}^{\otimes n}(\mathbf{z})}\right) \mathbb{1}\left\{Q_{\alpha_n}^{\otimes n}(\mathbf{z}) < Q_{\emptyset}^{\otimes n}(\mathbf{z})\right\}\right) \tag{3.155}$$

$$\overset{(a)}{\leqslant} \sum_{\mathbf{z}} \left|\widehat{Q}^n(\mathbf{z}) - Q_{\alpha_n}^{\otimes n}(\mathbf{z})\right| \left(n \log \frac{1}{\nu_{\min}} \mathbb{1}\left\{Q_{\alpha_n}^{\otimes n}(\mathbf{z}) \geqslant Q_{\emptyset}^{\otimes n}(\mathbf{z})\right\}\right.$$

$$\left. + \sum_{i=1}^{n} \log \frac{Q_{\emptyset}(z_i)}{\left(\prod_{k\in\mathcal{K}} (1-\rho_k\alpha_n)\right) Q_{\emptyset}(z_i)} \mathbb{1}\left\{Q_{\alpha_n}^{\otimes n}(\mathbf{z}) < Q_{\emptyset}^{\otimes n}(\mathbf{z})\right\}\right) \tag{3.156}$$

$$\leqslant \sum_{\mathbf{z}} \left|\widehat{Q}^n(\mathbf{z}) - Q_{\alpha_n}^{\otimes n}(\mathbf{z})\right| \left(n \log \frac{1}{\nu_{\min}} + n \log \frac{1}{\prod_{k\in\mathcal{K}} (1-\rho_k\alpha_n)}\right) \tag{3.157}$$

$$= 2\mathbb{V}\Big(\widehat{Q}^n, Q_{\alpha_n}^{\otimes n}\Big) \left(n \log \frac{1}{\left(\prod_{k\in\mathcal{K}} (1-\rho_k\alpha_n)\right) \nu_{\min}} \right) \tag{3.158}$$

$$\leqslant 2 \exp\left(-\frac{1}{2}\xi_2 n\alpha_n\right) \left(n \log \frac{1}{\left(\prod_{k\in\mathcal{K}} (1-\rho_k\alpha_n)\right) \nu_{\min}} \right), \tag{3.159}$$

where (a) follows from the fact that $Q_{\alpha_n}(z) \geqslant \prod_{k\in\mathcal{K}} (1-\rho_k\alpha_n)\, Q_\emptyset(z)$.

CHAPTER 4
EMBEDDING COVERT INFORMATION IN INNOCENT TRANSMISSIONS

4.1 Summary

In this chapter, we analyze a two-receiver binary-input discrete memoryless broadcast channel, in which the transmitter communicates a common message simultaneously to both receivers and a covert message to only one of them. The unintended recipient of the covert message is treated as an adversary who attempts to detect the covert transmission. This model captures the problem of embedding covert messages in an innocent codebook and generalizes previous covert communication models in which the innocent behavior corresponds to the absence of communication between legitimate users. We identify the exact asymptotic behavior of the number of covert bits that can be transmitted when the rate of the innocent codebook is close to the capacity of the channel to the adversary. Our results also identify the dependence of the number of covert bits on the channel parameters and the characteristics of the innocent codebook.

4.2 Introduction

As is customary, much of the literature on LPD communication define an innocent behavior in which the transmitter does not communicate. In contrast, in this chapter, we analyze a scenario in which the innocent behavior corresponds to the transmission of codewords from an innocent codebook that is permitted and decoded by the adversary. Since the definition of stealth communication is deceptively similar to that of covert communication, it is important to note the difference between them. Covert

communication, which is governed by the *square-root law*, is an extreme regime in which the adversary possesses the exact same knowledge as any other receiver except the secret key, if any. Hence, the adversary also knows the channel to expect when there is no input. However, in stealth communication, the adversary expects one channel when the true channel is another, and the stealth transmitter takes advantage of this to transmit with a linear rate. The work of Dutta *et al.* [77] on covert communication using dirty constellations is one of the motivations for our work in this chapter. In [77], the authors rely on channel noise to hide a covert signal by superimposing it on top of an innocent signal while incurring minimal distortion; consequently, the informed receiver can decode the covert message while the uninformed adversary attributes the distortion of the signal to channel impairments and hardware imperfections. Although the authors show that their message-hiding scheme is immune to certain statistical tests, their scheme is not fundamentally covert against a more powerful adversary. Our objective is to develop an information-theoretic analysis of embedding covert signals in innocent communication signals while escaping detection from an adversary who is not restricted to using a small set of statistical tests.

We model the setup of [77] as a two-user discrete memoryless broadcast channel in which a common message is sent to both users while a covert message is sent to only one user, treating the other as an adversary. This can be viewed as an instance of steganography [8], in which the covertext is controlled in part through the design of a coding scheme and in part through the channel noise that is only statistically known. The model that is closest to the one considered in this chapter is that of [35], which analyzes the same broadcast setup for BSCs and exploits the additive nature of the noise in BSCs. Our results generalize [35] using different proof techniques. Another related but different model is that of [78] in which the transmitter simultaneously sends two different covert messages to two legitimate users while escaping detection

from a third user. The authors have shown that time-division transmission is then optimal in certain cases. Although there exist technical and conceptual connections between our model and that of [78], our model captures a different problem and the results cannot be directly compared.

We build upon the channel resolvability techniques developed in [27, 69] for point-to-point channels and MACs, respectively, to embed covert information into innocent transmissions. As expected, we show that the transmitter can perturb no more than $\mathcal{O}(\sqrt{n})$ symbols of the n-length sequences representing the innocent transmission to be covert from the adversary. We precisely characterize the asymptotic behavior of the number of covert bits that can be transmitted when the rate of the innocent transmission approaches the capacity of the channel to the adversary. Our results highlight the dependence of the number of covert bits on the channel parameters and the characteristics of the innocent codebook.

The remainder of this chapter is organized as follows. In Section 4.3, we formally introduce our channel model, and in Section 4.4, we develop a preliminary result that captures the essence of our approach to embedding covert information in innocent transmissions. We present our main result in Section 4.5, which consists in an achievability and a converse characterizing the optimal asymptotic number of reliable and covert bits when the rate of the common message is close to the capacity of the channel to the adversary. Finally, we conclude our work in Section 4.6 with a brief discussion about extending our result to non-binary input alphabets. Proofs of lemmas are relegated to the appendix. This chapter is based on the results obtained in [79, 80].

4.3 Channel model

We analyze a channel model in which Alice, the transmitter, communicates a common message to both Bob, the receiver, and Willie, the warden, and a covert message

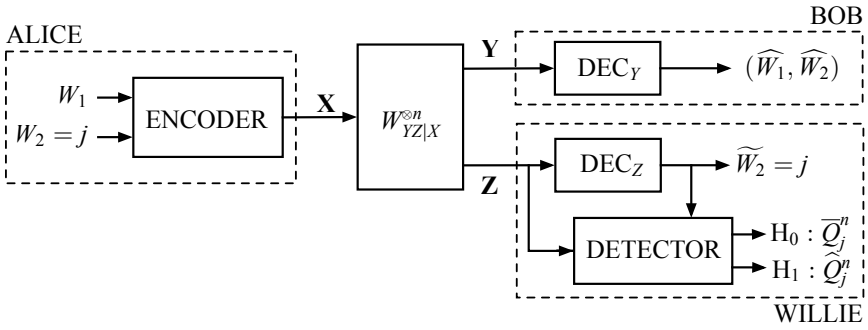

Figure 4.1: Model of covert communication over a discrete memoryless broadcast channel for a fixed common message $W_2 = j$.

to Bob alone over a discrete memoryless broadcast channel $\left(\mathcal{X}, W_{YZ|X}, \mathcal{Y}, \mathcal{Z}\right)$. We assume that the transmitter uses a binary input alphabet $\mathcal{X} \triangleq \{0, 1\}$ and that the output alphabets $\mathcal{Y}$ and $\mathcal{Z}$ are finite. Furthermore, we assume that all terminals are synchronized and possess complete knowledge of the coding scheme used.

As illustrated in Figure 4.1, Alice wishes to communicate a uniformly distributed common message $W_2 \in [\![1, M_2]\!]$ to both Bob and Willie, and a uniformly distributed covert message $W_1 \in [\![1, M_1]\!]$ to Bob alone in n channel uses. Alice may also choose not to transmit any covert message, in which case, she sets $W_1 = 0$. Note that there is no prior on whether $W_1 = 0$ or $W_1 \neq 0$. Alice then encodes the message pair $(W_1, W_2) = (i, j)$ into an n-length codeword $\mathbf{X}_{ij}$. We label the collection of codewords $\{\mathbf{X}_{0j}\}_{j=1}^{M_2}$ as the *innocent codebook*. Alice sends the codeword over the discrete memoryless broadcast channel in n channel uses, at the end of which, Bob and Willie observe the n-length sequences $\mathbf{Y}$ and $\mathbf{Z}$, respectively. Since the channel is memoryless, we denote the transition probability corresponding to n uses of the channel by $W_{YZ|X}^{\otimes n} \triangleq \prod_{i=1}^{n} W_{YZ|X}$. For $a \in \mathcal{X}$, we denote the output distributions induced by each input symbol at Bob and Willie by $P_a(y) \triangleq W_{Y|X}(y|a)$ and $Q_a(z) \triangleq W_{Z|X}(z|a)$, respectively. For $a, b \in \mathcal{X}$ with $a \neq b$, we assume $P_a \ll P_b$, $Q_a \ll Q_b$, $Q_a \neq Q_b$. Without the first assumption, Bob has an unfair advantage over Willie [27]. Without the second and third assumptions, achieving covert communication is either impossible or trivial [27, 33]. In addition, we make the following assumptions as well.

- The channel $\left(\mathcal{X}, W_{Z|X}, \mathcal{Z}\right)$ to Willie admits a unique capacity-achieving input distribution Λ, for which $\Lambda(1) \triangleq \lambda^*$, where $\lambda^* > 0$. Many channels encountered in practice satisfy this assumption.[1]

- $\mathbb{I}\left(\Lambda, W_{Y|X}\right) \geqslant \mathbb{I}\left(\Lambda, W_{Z|X}\right)$, so that Willie limits the rate of the common message.

Upon observing the noisy sequence $\mathbf{Z}$, Willie forms an estimate $\widetilde{W}_2$ of W_2. We measure reliability at Willie using the following metric,

$$P_e^{(2)} \triangleq \frac{1}{M_2} \sum_{j=1}^{M_2} P_{e,j}^{(2)} = \mathbb{E}_{W_2}\left(P_{e,W_2}^{(2)}\right), \tag{4.1}$$

where

$$P_{e,j}^{(2)} \triangleq \mathbb{P}\Big(\widetilde{W}_2 \neq j | W_1 = 0, W_2 = j\Big) + \mathbb{P}\Big(\widetilde{W}_2 \neq j | W_1 \neq 0, W_2 = j\Big). \tag{4.2}$$

Willie attempts to detect the presence of a non-zero covert message by performing a binary-hypothesis test on his observation $\mathbf{Z}$ to distinguish between hypotheses $H_0 \triangleq \{W_1 = 0\}$ and $H_1 \triangleq \{W_1 \neq 0\}$. We denote Willie's Type I and Type II error probabilities by α and β, respectively. For a fixed $W_2 = j$, the output distribution observed by Willie is

$$\overline{Q}_j^n(\mathbf{z}) \triangleq W_{Z|X}^{\otimes n}\left(\mathbf{z}|\mathbf{x}_{0j}\right), \quad \text{if } W_1 = 0, \tag{4.3}$$

$$\widehat{Q}_j^n(\mathbf{z}) \triangleq \frac{1}{M_1} \sum_{i=1}^{M_1} W_{Z|X}^{\otimes n}\left(\mathbf{z}|\mathbf{x}_{ij}\right), \quad \text{otherwise.} \tag{4.4}$$

For a fixed common message $W_2 = j$, we measure the covertness of W_1 by the KL divergence $\mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big)$. Note that any statistical test [28] conducted on $\mathbf{Z}$ by Willie must satisfy $\alpha + \beta \geqslant 1 - \mathbb{V}\Big(\widehat{Q}_j^n, \overline{Q}_j^n\Big)$. Using Pinsker's inequality [26], we write

[1] Note that this assumption is only required to prove the converse.

$\alpha + \beta \geqslant 1 - \sqrt{\mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big)}$. Consequently , a vanishing KL divergence ensures that $\alpha + \beta = 1$ in the limit so that Willie's statistical test is no better than a random guess.

Upon observing $\mathbf{Y}$, Bob forms an estimate $(\widehat{W}_1, \widehat{W}_2)$ of the transmitted message pair (W_1, W_2). We measure reliability at Bob using the metric

$$P_e^{(1)} \triangleq \frac{1}{M_2} \sum_{j=1}^{M_2} \left(P_{e,1,j}^{(1)} + P_{e,2,j}^{(1)} \right), \tag{4.5}$$

$$= \mathbb{E}_{W_2} \left(P_{e,1,W_2}^{(1)} \right) + \mathbb{E}_{W_2} \left(P_{e,2,W_2}^{(1)} \right), \tag{4.6}$$

where

$$\begin{aligned} P_{e,1,j}^{(1)} &\triangleq \mathbb{P}\Big(\widehat{W}_1 \neq 0 | W_1 = 0, \widehat{W}_2 = W_2 = j\Big) \\ &\quad + \mathbb{P}\Big(\widehat{W}_1 \neq W_1 | W_1 \neq 0, \widehat{W}_2 = W_2 = j\Big), \end{aligned} \tag{4.7}$$

$$\begin{aligned} P_{e,2,j}^{(1)} &\triangleq \mathbb{P}\Big(\widehat{W}_2 \neq j | W_1 = 0, W_2 = j\Big) \\ &\quad + \mathbb{P}\Big(\widehat{W}_2 \neq j | W_1 \neq 0, W_2 = j\Big). \end{aligned} \tag{4.8}$$

Definition 2. *A code for the above model is an* $(M_1, M_2, n, \epsilon, \delta)$ *code if* $P_e^{(1)} \leqslant \epsilon$, $P_e^{(2)} \leqslant \epsilon$, *and* $\mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big) \leqslant \delta$ *for all* $j \in [\![1, M_2]\!]$.

Note that $P_e^{(1)}$ and $P_e^{(2)}$ are not usual average error probabilities because our model does not impose a prior on whether Alice embeds a covert message or not. Nevertheless, one can check from the definition that a small values of $P_e^{(1)}$ and $P_e^{(2)}$ guarantee that the average error probability of Bob and Willie is small. Also note that we choose to satisfy the stringent requirement that $\lim_{n\to\infty} \mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big)$ vanishes *for every* $j \in [\![1, M_2]\!]$ so that the hypothesis test used by Willie is futile in detecting the presence of any covert message for *every choice* of the common message and not just on average.

Definition 3. *A throughput/rate pair (r_1, r_2) is achievable if there exists a sequence of $(M_1, M_2, n, \epsilon_n, \delta_n)$ codes*[2] *with increasing blocklength n such that for all $j \in [\![1, M_2]\!]$,*

$$r_1 \leqslant \liminf_{n\to\infty} \frac{\log M_1}{\sqrt{n\mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big)}}, \tag{4.9}$$

$$r_2 \leqslant \liminf_{n\to\infty} \frac{\log M_2}{n}, \tag{4.10}$$

and

$$\lim_{n\to\infty} \epsilon_n = \lim_{n\to\infty} \delta_n = 0. \tag{4.11}$$

The optimal covert throughput is the supremum of all covert throughputs r_1 that can be achieved when the common message is transmitted at a rate close to the capacity of the channel to Willie.

A couple of comments are now in order. First, note that our goal is twofold here.

- We wish to design a reliable code to communicate a common message and a reliable code to embed a covert message; this is a *joint* code-design problem, and we do not address the problem of embedding covert bits into a fixed code for the common message.

- Our problem generalizes previous works on covert communication, in which covertness was measured w.r.t. the innocent distribution $Q_0^{\otimes n}$ corresponding to the transmission of the all-zero sequence. In our case, for $W_2 = j \in [\![1, M_2]\!]$, covertness is measured w.r.t. the distribution $\overline{Q}_j^n$, which is a product distribution that is *not identically distributed* and corresponds to the communication of the innocent codeword mapped to the common message $W_2 = j$.

[2]Note that we only consider communication schemes for which $\lim_{n\to\infty} \log M_1 = \infty$.

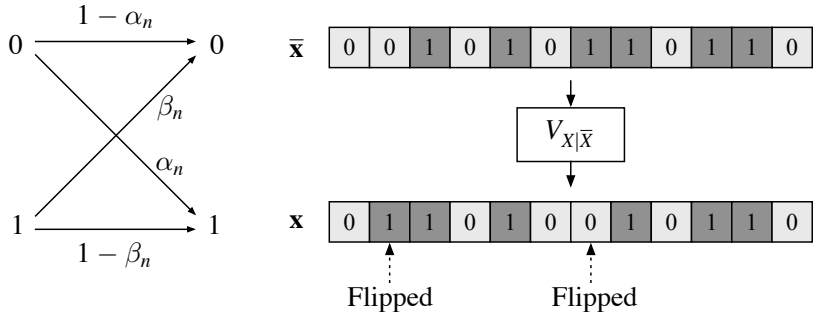

Figure 4.1: Binary asymmetric channel $V_{X|\overline{X}}$ and an illustration of innocent symbols flipped by the channel $V_{X|\overline{X}}$.

4.4 Preliminaries

Similar to our approach in Chapter 3, we define a *covert stochastic process*, which serves as the target distribution that our covert code approximates. In this case, by introducing the covert process, we precisely quantify the fraction of symbols in the innocent codeword that Alice can perturb to transmit covert information while simultaneously avoiding detection by Willie.

For a fixed $n \in \mathbb{N}^*$ and a sequence $\overline{\mathbf{x}} \in \mathcal{X}^n$, we define the covert process as the output of the binary asymmetric channel $V_{X|\overline{X}}$ illustrated in Figure 4.1 such that $V_{X|\overline{X}}(1|0) \triangleq \alpha_n$ and $V_{X|\overline{X}}(0|1) \triangleq \beta_n$, where $\alpha_n, \beta_n \in (0,1)$ are cross-over probabilities. We denote the input distribution of the covert process by $\Pi_{\overline{\mathbf{x}},\alpha_n,\beta_n}$ defined as

$$\Pi_{\overline{\mathbf{x}},\alpha_n,\beta_n}(\mathbf{x}) \triangleq \prod_{i=1}^{n} V_{X|\overline{X}}\left(x_i|\overline{x}_i\right). \tag{4.12}$$

We set $\gamma_n \triangleq \frac{\beta_n}{\alpha_n}$, and when defining a sequence $\{\gamma_n\}_{n\in\mathbb{N}^*}$, we ask that it converges to $\gamma \in \mathbb{R}^+$. As a result, we induce the output distributions

$$\overline{P}^{\otimes n}_{\overline{\mathbf{x}},\alpha_n,\beta_n}(\mathbf{y}) \triangleq \sum_{\mathbf{x}} W^{\otimes n}_{Y|X}\left(\mathbf{y}|\mathbf{x}\right) \Pi_{\overline{\mathbf{x}},\alpha_n,\beta_n}(\mathbf{x}), \tag{4.13}$$

$$\overline{Q}^{\otimes n}_{\overline{\mathbf{x}},\alpha_n,\beta_n}(\mathbf{z}) \triangleq \sum_{\mathbf{x}} W^{\otimes n}_{Z|X}\left(\mathbf{z}|\mathbf{x}\right) \Pi_{\overline{\mathbf{x}},\alpha_n,\beta_n}(\mathbf{x}), \tag{4.14}$$

at Bob and Willie, respectively. Note that both $\overline{P}^{\otimes n}_{\overline{\mathbf{x}},\alpha_n,\beta_n}$ and $\overline{Q}^{\otimes n}_{\overline{\mathbf{x}},\alpha_n,\beta_n}$ are product distributions, and setting both cross-over probabilities, α_n and β_n, to 0 results in a distribution $\overline{Q}^{\otimes n}_{\overline{\mathbf{x}},0,0}$ at Willie. We now have the following generalization of [27, Lemma 1].

Lemma 8. *Let $\alpha_n, \beta_n \in (0,1)$ be such that $\lim_{n\to\infty} \alpha_n = \lim_{n\to\infty} \beta_n = 0$. Let $\overline{\mathbf{x}} \in \mathcal{X}^n$ and set $\lambda_n \triangleq \sum_{i=1}^{n} \frac{\mathbb{1}\{\overline{x}_i=1\}}{n}$. Then, for a large $n \in \mathbb{N}^*$, we bound $\mathbb{D}\big(\overline{Q}^{\otimes n}_{\overline{\mathbf{x}},\alpha_n,\beta_n} \| \overline{Q}^{\otimes n}_{\overline{\mathbf{x}},0,0}\big)$ by*

$$\begin{aligned} n\bigg((1-\lambda_n)\frac{\alpha_n^2}{2}\left(1+\sqrt{\alpha_n}\right)\chi_2\left(Q_1\|Q_0\right)+\lambda_n\frac{\beta_n^2}{2}\Big(1+\sqrt{\beta_n}\Big)\chi_2\left(Q_0\|Q_1\right)\bigg) &\geqslant \mathbb{D}\big(\overline{Q}^{\otimes n}_{\overline{\mathbf{x}},\alpha_n,\beta_n} \| \overline{Q}^{\otimes n}_{\overline{\mathbf{x}},0,0}\big) \\ &\geqslant n\left((1-\lambda_n)\,\frac{\alpha_n^2}{2}\left(1-\sqrt{\alpha_n}\right)\chi_2\left(Q_1\|Q_0\right)+\lambda_n\frac{\beta_n^2}{2}\Big(1-\sqrt{\beta_n}\Big)\,\chi_2\left(Q_0\|Q_1\right)\right). \end{aligned} \tag{4.15}$$

The proof of Lemma 8 is provided in Appendix 4.A. For any $\overline{\mathbf{x}}$, upon choosing sequences $\{\alpha_n\}_{n\in\mathbb{N}^*}$ and $\{\beta_n\}_{n\in\mathbb{N}^*}$ such that $\lim_{n\to\infty} n\alpha_n^2 = \lim_{n\to\infty} n\beta_n^2 = 0$, we obtain

$$\lim_{n\to\infty} \mathbb{D}\big(\overline{Q}^{\otimes n}_{\overline{\mathbf{x}},\alpha_n,\beta_n} \| \overline{Q}^{\otimes n}_{\overline{\mathbf{x}},0,0}\big) = 0, \tag{4.16}$$

which implies $\overline{Q}^{\otimes n}_{\overline{\mathbf{x}},\alpha_n,\beta_n}$ is indistinguishable from $\overline{Q}^{\otimes n}_{\overline{\mathbf{x}},0,0}$ at Willie. In addition, it is also possible to simultaneously choose sequences $\{\alpha_n\}_{n\in\mathbb{N}^*}$ and $\{\beta_n\}_{n\in\mathbb{N}^*}$ such that $\lim_{n\to\infty} n\alpha_n = \lim_{n\to\infty} n\beta_n = \infty$ to flip an infinite number of innocent symbols as $n \to \infty$, while still ensuring that $\overline{Q}^{\otimes n}_{\overline{\mathbf{x}},\alpha_n,\beta_n}$ is indistinguishable from $\overline{Q}^{\otimes n}_{\overline{\mathbf{x}},0,0}$ according to (4.15). If we set $\overline{\mathbf{x}} = \mathbf{x}_{0j}$, where $\mathbf{x}_{0j}$ is the innocent codeword corresponding to $W_2 = j$, the distribution $\overline{Q}^{\otimes n}_{\mathbf{x}_{0j},0,0}$ is the innocent distribution corresponding to transmitting just the common message $W_2 = j$ and is equivalent to the distribution $\overline{Q}_j^n$ in (4.3).

4.5 Main result

We now characterize the exact scaling of the number of covert bits when the common message is transmitted at a rate approaching the capacity of the channel to Willie. Also, for the transmission of covert bits without a secret key, Bob is required to possess a certain advantage over Willie, which we precisely characterize in the following theorem.

Theorem 3. *For the channel model described in Section 4.3, if there exists a* $\gamma \geqslant 0$ *such that*

$$(1-\lambda^*)\,\mathbb{D}(P_1\|P_0) + \lambda^*\gamma\mathbb{D}(P_0\|P_1) > (1-\lambda^*)\,\mathbb{D}(Q_1\|Q_0) + \lambda^*\gamma\mathbb{D}(Q_0\|Q_1), \quad (4.17)$$

for the λ^* *defined in Section 4.3, then the throughput/rate pair* (r_1, r_2) *given by*

$$r_1 = \max_{\gamma\geqslant 0} (1-\mu)\,\frac{\sqrt{2}\left((1-\lambda^*)\,\mathbb{D}(P_1\|P_0) + \lambda^*\gamma\mathbb{D}(P_0\|P_1)\right)}{\sqrt{(1-\lambda^*)\,\chi_2\left(Q_1\|Q_0\right) + \lambda^*\gamma^2\chi_2\left(Q_0\|Q_1\right)}}, \quad (4.18)$$

$$r_2 = (1-\mu)\,\mathbb{I}\left(\Lambda, W_{Z|X}\right), \quad (4.19)$$

where the maximum in (4.18) *is over all* γ *that satisfy* (4.17)*, is achievable.*[3]

Proof. We first show that Bob can decode the covert message, and both Bob and Willie can decode the common message reliably. Using channel resolvability techniques, we then show that the induced distribution $\widehat{Q}^n_{W_2}$ corresponding to the common message W_2 is indistinguishable from the covert stochastic process $\overline{Q}^{\otimes n}_{\mathbf{x}_{0W_2},\alpha_n,\beta_n}$ when averaged over all choices of the common message W_2. Finally, we identify a coding scheme that achieves (4.18) and (4.19) such that (4.17) is satisfied.

[3]Note that the characterization of r_1 in (4.18) is valid for all $\lambda \in [0,1]$ and not just λ^*, as long as there exists a $\gamma \geqslant 0$ that satisfies $(1-\lambda)\,\mathbb{D}(P_1\|P_0) + \lambda\gamma\mathbb{D}(P_0\|P_1) > (1-\lambda)\,\mathbb{D}(Q_1\|Q_0) + \lambda\gamma\mathbb{D}(Q_0\|Q_1)$.

Random code generation Let us define a set $\mathcal{D}_\epsilon^n \triangleq \{\mathbf{x} : |\frac{\mathrm{wt}(\mathbf{x})}{n} - \lambda^*| < \epsilon\}$, where $\mathrm{wt}(\mathbf{x}) \triangleq |\ell \in [\![1, n]\!] : x_\ell = 1|$ is the weight of $\mathbf{x}$. For $j \in [\![1, M_2]\!]$, we generate M_2 codewords $\mathbf{x}_{0j} \in \mathcal{X}^n$ independently at random according to the distribution P_X^n defined by

$$P_X^n(\mathbf{x}) \triangleq \frac{\Lambda^{\otimes n}(\mathbf{x})\, \mathbb{1}\{\mathbf{x} \in \mathcal{D}_\epsilon^n\}}{\mathbb{P}_{\Lambda^{\otimes n}}(\mathbf{X} \in \mathcal{D}_\epsilon^n)}. \tag{4.20}$$

Generating $\{\mathbf{x}_{0j}\}_{j=1}^{M_2}$ according to P_X^n ensures that every $\mathbf{x}_{0j}$ is ϵ-letter typical w.r.t. the distribution Λ. We label this set of M_2 codewords as the innocent codebook $\mathcal{C}_2$. For every $W_2 = j \in [\![1, M_2]\!]$, we generate M_1 codewords independently at random according to the distribution $\Pi_{\mathbf{x}_{0j}, \alpha_n, \beta_n}$ and label this set of codewords as the covert sub-codebook $\mathcal{C}_{1,j}$ corresponding to the common message $W_2 = j$. Alice encodes the message pair $(W_1, W_2) = (i, j)$, where $i \in [\![1, M_1]\!]$ and $j \in [\![1, M_2]\!]$, to the codeword $\mathbf{x}_{ij} \in \mathcal{C}_{1,j}$ and transmits it through the discrete memoryless broadcast channel. Defining

$$W_{Y|\overline{X}}(y|\overline{x}) \triangleq \sum_x W_{Y|X}(y|x) V_{X|\overline{X}}(x|\overline{x}), \tag{4.21}$$

$$W_{Z|\overline{X}}(z|\overline{x}) \triangleq \sum_x W_{Z|X}(z|x) V_{X|\overline{X}}(x|\overline{x}), \tag{4.22}$$

we show that the decoding error probability of the common message at Bob and Willie averaged over all random codebooks $\mathcal{C}$ decays exponentially in the following lemma.

Lemma 9. *For any $\mu \in (0, 1), \exists\, n_0 \in \mathbb{N}^*$ such that for all $n \geqslant n_0$, if*

$$\log M_2 \leqslant (1 - \mu)\, n \min\left(\mathbb{I}\Big(\Lambda, W_{Y|\overline{X}}\Big), \mathbb{I}\Big(\Lambda, W_{Z|\overline{X}}\Big)\right), \tag{4.23}$$

we have

$$\mathbb{E}_{\mathcal{C}}\left(\mathbb{E}_{W_2} P^{(1)}_{e,2,W_2}\right) \leqslant \exp\left(-\xi_1 n\right), \tag{4.24}$$

$$\mathbb{E}_{\mathcal{C}}\left(\mathbb{E}_{W_2} P^{(2)}_{e,W_2}\right) \leqslant \exp\left(-\xi_1 n\right), \tag{4.25}$$

for an appropriate constant $\xi_1 > 0$.

The proof of Lemma 9 follows the random coding argument outlined in [81, Section 7.3] and is omitted here. Note that $\forall(\overline{x}, z) \in \mathcal{X} \times \mathcal{Z}$,

$$W_{Z|\overline{X}}(z|\overline{x}) = V_{X|\overline{X}}(0|\overline{x}) Q_0(z) + V_{X|\overline{X}}(1|\overline{x}) Q_1(z). \tag{4.26}$$

Consequently, we have

$$W_{Z|\overline{X}}(z|0) = Q_0(z) + \alpha_n \left(Q_1(z) - Q_0(z)\right), \tag{4.27}$$

$$W_{Z|\overline{X}}(z|1) = Q_1(z) + \beta_n \left(Q_0(z) - Q_1(z)\right). \tag{4.28}$$

Since $\lim_{n\to\infty} \alpha_n = \lim_{n\to\infty} \beta_n = 0$, the channels $W_{Z|\overline{X}}$ and $W_{Z|X}$ are identical in the limit of large blocklength. Using a similar argument, we can show that the channels $W_{Y|\overline{X}}$ and $W_{Y|X}$ are identical in the limit of large blocklength.

Next, defining $Q_Z(z) \triangleq \sum_{\overline{x}} \Lambda(\overline{x}) W_{Z|\overline{X}}(z|\overline{x})$ and expanding the mutual information

term $\mathbb{I}\Big(\Lambda, W_{Z|\overline{X}}\Big)$ using (4.27) and (4.28), we obtain

$$\begin{aligned}
&\mathbb{I}\Big(\Lambda, W_{Z|\overline{X}}\Big) \\
&\quad= \sum_z \Bigg((1-\lambda^*)\left(Q_0(z)+\alpha_n\left(Q_1(z)-Q_0(z)\right)\right) \log\left(\frac{Q_0(z)+\alpha_n\left(Q_1(z)-Q_0(z)\right)}{Q_Z(z)}\right) \\
&\qquad + \lambda^*\left(Q_1(z)+\beta_n\left(Q_0(z)-Q_1(z)\right)\right) \log\left(\frac{Q_1(z)+\beta_n\left(Q_0(z)-Q_1(z)\right)}{Q_Z(z)}\right)\Bigg)
\end{aligned} \tag{4.29}$$

$$= \sum_z \left((1-\lambda^*) Q_0(z) \log \frac{Q_0(z)}{Q_Z(z)} + \lambda^* Q_1(z) \log \frac{Q_1(z)}{Q_Z(z)} \right) + \mathcal{O}(\alpha_n) + \mathcal{O}(\beta_n) \tag{4.30}$$

$$= \mathbb{I}\big(\Lambda, W_{Z|X}\big) + \mathcal{O}(\alpha_n) + \mathcal{O}(\beta_n). \tag{4.31}$$

Similarly, we obtain

$$\mathbb{I}\Big(\Lambda, W_{Y|\overline{X}}\Big) = \mathbb{I}\big(\Lambda, W_{Y|X}\big) + \mathcal{O}(\alpha_n) + \mathcal{O}(\beta_n). \tag{4.32}$$

Using (4.31) and (4.32), we rewrite the condition in (4.23) as

$$\frac{\log M_2}{n} \leqslant (1-\mu) \min\left(\mathbb{I}\big(\Lambda, W_{Y|X}\big) + \mathcal{O}(\alpha_n) + \mathcal{O}(\beta_n), \mathbb{I}\big(\Lambda, W_{Z|X}\big) + \mathcal{O}(\alpha_n) + \mathcal{O}(\beta_n) \right). \tag{4.33}$$

Recall our assumption that $\mathbb{I}\left(\Lambda, W_{Y|X}\right) \geqslant \mathbb{I}\left(\Lambda, W_{Z|X}\right)$ in Section 4.3 and the fact that $\lim_{n\to\infty} \alpha_n = \lim_{n\to\infty} \beta_n = 0$. Consequently, we assume both Bob and Willie have decoded the common message successfully and set

$$\lim_{n\to\infty} \frac{\log M_2}{n} = (1-\mu)\, \mathbb{I}\big(\Lambda, W_{Z|X}\big), \tag{4.34}$$

for an arbitrary $\mu \in (0,1)$.

Channel reliability analysis We now prove that the decoding error probability of the covert message at Bob decays exponentially. For $i \in [\![1, M_1]\!]$, the following events lead to a decoding error at Bob,

- codeword $\mathbf{x}_{0j}$ is transmitted, and the decoder incorrectly estimates $\widehat{W}_1 = i$,
- codeword $\mathbf{x}_{ij}$ is transmitted, and the decoder incorrectly estimates $\widehat{W}_1 = 0$,
- codeword $\mathbf{x}_{ij}$ is transmitted, and the decoder incorrectly estimates $\widehat{W}_1 = i' \in [\![1, M_1]\!]$, where $i' \neq i$.

The decoding error probability of the covert message at Bob averaged over all random codebooks satisfies the following lemma.

Lemma 10. *For any $\mu \in (0,1)$, $\exists\, n_0 \in \mathbb{N}^*$ such that for all $n \geqslant n_0$, if*

$$\log M_1 = (1-\mu)n((1-\lambda^*)\,\alpha_n \mathbb{D}(P_1 \| P_0) + \lambda^* \beta_n \mathbb{D}(P_0 \| P_1)), \tag{4.35}$$

we have

$$\mathbb{E}_{\mathcal{C}}\left(\mathbb{E}_{W_2} P^{(1)}_{e,1,W_2}\right) \leqslant \exp\left(-\xi_2 n \alpha_n\right) + \exp\left(-\xi_2 n \beta_n\right), \tag{4.36}$$

for an appropriate $\xi_2 > 0$.

The proof of Lemma 10 is provided in Appendix 4.B.

Channel resolvability analysis We now show that the KL divergence between the induced distribution $\widehat{Q}^n_{W_2}$ and the covert stochastic process $\overline{Q}^{\otimes n}_{\mathbf{X}_{0W_2},\alpha_n,\beta_n}$ averaged over all choices of the common message and all random codebooks vanishes in the limit of large blocklength.

Lemma 11. *For any $\nu > 0$, $\exists\, n_0 \in \mathbb{N}^*$ such that for all $n \geqslant n_0$, if*

$$\log M_1 = (1+\nu) n ((1-\lambda^*)\, \alpha_n \mathbb{D}(Q_1 \| Q_0) + \lambda^* \beta_n \mathbb{D}(Q_0 \| Q_1)), \tag{4.37}$$

we have

$$\mathbb{E}_{\mathcal{C}}\Big(\mathbb{E}_{W_2}\mathbb{D}\Big(\widehat{Q}^n_{W_2} \| \overline{Q}^{\otimes n}_{\mathbf{X}_{0W_2},\alpha_n,\beta_n}\Big)\Big) \leqslant \exp\left(-\xi_3 n \alpha_n\right) + \exp\left(-\xi_3 n \beta_n\right), \tag{4.38}$$

for an appropriate $\xi_3 > 0$.

The proof of Lemma 11 is provided in Appendix 4.C.

Identification of a specific code Using Markov's inequality, we obtain

$$\begin{aligned}\mathbb{P}\Bigg(& \mathbb{E}_{W_2} P^{(1)}_{e,1,W_2} < 8\mathbb{E}_{\mathcal{C}}\left(\mathbb{E}_{W_2} P^{(1)}_{e,1,W_2}\right) \bigcap \mathbb{E}_{W_2} P^{(1)}_{e,2,W_2} < 8\mathbb{E}_{\mathcal{C}}\left(\mathbb{E}_{W_2} P^{(1)}_{e,2,W_2}\right) \\ & \bigcap \mathbb{E}_{W_2}\mathbb{D}\Big(\widehat{Q}^n_{W_2} \| \overline{Q}^{\otimes n}_{\mathbf{x}_{0W_2},\alpha_n,\beta_n}\Big) < 8\mathbb{E}_{\mathcal{C}}\Big(\mathbb{E}_{W_2}\mathbb{D}\Big(\widehat{Q}^n_{W_2} \| \overline{Q}^{\otimes n}_{\mathbf{X}_{0W_2},\alpha_n,\beta_n}\Big)\Big) \\ & \bigcap \mathbb{E}_{W_2} P^{(2)}_{e,W_2} < 8\mathbb{E}_{\mathcal{C}}\left(\mathbb{E}_{W_2} P^{(2)}_{e,W_2}\right)\Bigg) \geqslant \frac{1}{2}. \end{aligned} \tag{4.39}$$

Defining $\epsilon_n \triangleq \exp\left(-\xi_4 n \alpha_n\right) + \exp\left(-\xi_4 n \beta_n\right)$ for an appropriate constant $\xi_4 > 0$, we conclude from (4.39) that there exists at least one coding scheme $\mathcal{C}^*$ such that for a large n,

$$\mathbb{E}_{W_2} P^{(1)}_{e,1,W_2} \leqslant \epsilon_n, \tag{4.40}$$

$$\mathbb{E}_{W_2} P^{(1)}_{e,2,W_2} \leqslant \epsilon_n, \tag{4.41}$$

$$\mathbb{E}_{W_2} P^{(2)}_{e,W_2} \leqslant \epsilon_n, \tag{4.42}$$

$$\mathbb{E}_{W_2}\mathbb{D}\Big(\widehat{Q}^n_{W_2} \| \overline{Q}^{\otimes n}_{\mathbf{x}_{0W_2},\alpha_n,\beta_n}\Big) \leqslant \epsilon_n, \tag{4.43}$$

where $\mathbf{x}_{0W_2} \in \mathcal{C}_2^*$ is the codeword corresponding to the common message W_2. We expurgate half of the innocent codewords and their corresponding covert sub-codebooks such that for every remaining $W_2 = j$, we have

$$P_{e,1,j}^{(1)} \leqslant 8\epsilon_n, \tag{4.44}$$

$$P_{e,2,j}^{(1)} \leqslant 8\epsilon_n, \tag{4.45}$$

$$P_{e,j}^{(2)} \leqslant 8\epsilon_n, \tag{4.46}$$

$$\mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}\Big) \leqslant 8\epsilon_n, \tag{4.47}$$

without affecting the asymptotic rate of the common message. Note that covertness is not affected by expurgating whole covert sub-codebooks. Since $\lim_{n\to\infty} \epsilon_n = 0$, (4.44), (4.45), and (4.46) imply $\lim_{n\to\infty} P_e^{(1)} = \lim_{n\to\infty} P_e^{(2)} = 0$.

Using Pinsker's inequality with (4.47), we have $\mathbb{V}\Big(\widehat{Q}_j^n, \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}\Big) \leqslant \exp\left(-\xi_5 n\alpha_n\right) + \exp\left(-\xi_5 n\beta_n\right)$ for an appropriate $\xi_5 > 0$. Then, we write

$$\begin{aligned}\mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big) = \mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}\Big) + \mathbb{D}\Big(\overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n} \| \overline{Q}_{\mathbf{x}_{0j},0,0}^{\otimes n}\Big) \\ + \sum_{\mathbf{z}} \Big(\widehat{Q}_j^n(\mathbf{z}) - \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})\Big) \log \frac{\overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})}{\overline{Q}_{\mathbf{x}_{0j},0,0}^{\otimes n}(\mathbf{z})}.\end{aligned} \tag{4.48}$$

Following steps similar to [69, (249)-(254)], we bound the absolute value of the last term in (4.48) for a large n and an appropriate $\xi_6 > 0$ by

$$\left|\sum_{\mathbf{z}} \Big(\widehat{Q}_j^n(\mathbf{z}) - \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})\Big) \log \frac{\overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})}{\overline{Q}_{\mathbf{x}_{0j},0,0}^{\otimes n}(\mathbf{z})}\right| \leqslant \exp\left(-\xi_6 n\alpha_n\right) + \exp\left(-\xi_6 n\beta_n\right). \tag{4.49}$$

Combining (4.47) to (4.49), we conclude that for a large n,

$$\left|\mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big) - \mathbb{D}\Big(\overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n} \| \overline{Q}_{\mathbf{x}_{0j},0,0}^{\otimes n}\Big)\right| \leqslant \exp\left(-\xi_7 n\alpha_n\right) + \exp\left(-\xi_7 n\beta_n\right), \tag{4.50}$$

for an appropriate constant $\xi_7 > 0$.

Asymptotic behavior We now establish the asymptotic scaling of $\log M_1$ for the proposed covert communication scheme. Combining (4.15) and (4.50), for a fixed $W_2 = j$, we bound $\mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big)$ by

$$\mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big) \leqslant n \left((1-\lambda^*) \frac{\alpha_n^2}{2} \left(1 + \sqrt{\alpha_n}\right) \chi_2 \left(Q_1 \| Q_0\right) + \lambda^* \frac{\beta_n^2}{2} \left(1 + \sqrt{\beta_n}\right) \chi_2 \left(Q_0 \| Q_1\right) \right) + \exp\left(-\xi_7 n \alpha_n\right) + \exp\left(-\xi_7 n \beta_n\right), \tag{4.51}$$

$$\mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big) \geqslant n \left((1-\lambda^*) \frac{\alpha_n^2}{2} \left(1 - \sqrt{\alpha_n}\right) \chi_2 \left(Q_1 \| Q_0\right) + \lambda^* \frac{\beta_n^2}{2} \left(1 - \sqrt{\beta_n}\right) \chi_2 \left(Q_0 \| Q_1\right) \right) - \exp\left(-\xi_7 n \alpha_n\right) - \exp\left(-\xi_7 n \beta_n\right). \tag{4.52}$$

Combining (4.35), (4.51), and (4.52), we obtain

$$\lim_{n\to\infty} \frac{\log M_1}{\sqrt{n \mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big)}} = \sqrt{2}\,(1-\mu)\, \frac{(1-\lambda^*)\, \mathbb{D}(P_1 \| P_0) + \lambda^* \gamma \mathbb{D}(P_0 \| P_1)}{\sqrt{(1-\lambda^*)\, \chi_2\left(Q_1 \| Q_0\right) + \lambda^* \gamma^2 \chi_2\left(Q_0 \| Q_1\right)}}. \tag{4.53}$$

Ultimately, combining (4.37), (4.51), (4.52), and (4.53), we arrive at the condition in (4.17). □

Theorem 4. *For the channel model described in Section 4.3, consider a sequence of $(M_1, M_2, n, \epsilon_n, \delta_n)$ codes with increasing block length n such that $\lim_{n\to\infty} \epsilon_n = 0$ and $\lim_{n\to\infty} \delta_n = 0$. If the common message is transmitted using a codebook that achieves the capacity of the channel to Willie, then for every $j \in [\![1, M_2]\!]$, there exists an infinite subset $\mathcal{N} \subseteq \mathbb{N}^*$ such that*

$$\liminf_{\substack{n\to\infty \\ n\in\mathcal{N}}} \frac{\log M_1}{\sqrt{n \mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big)}} \leqslant \max_{\gamma \geqslant 0} \sqrt{2} \frac{(1-\lambda^*)\, \mathbb{D}(P_1 \| P_0) + \lambda^* \gamma \mathbb{D}(P_0 \| P_1)}{\sqrt{(1-\lambda^*)\, \chi_2\left(Q_1 \| Q_0\right) + \lambda^* \gamma^2 \chi_2\left(Q_0 \| Q_1\right)}}. \tag{4.54}$$

For some $\gamma^* \geqslant 0$ that maximizes the right hand side of (4.54) and for a subsequence

of codes with increasing blocklength $n \in \mathcal{N}$ that achieves a covert throughput equal to the right hand side of (4.54)*, we have*

$$\limsup_{\substack{n\to\infty \\ n\in\mathcal{N}}} \frac{\log M_1}{\sqrt{n\mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big)}} \geqslant \sqrt{2}\frac{(1-\lambda^*)\,\mathbb{D}(Q_1\|Q_0) + \lambda^*\gamma^*\mathbb{D}(Q_0\|Q_1)}{\sqrt{(1-\lambda^*)\,\chi_2\left(Q_1\|Q_0\right) + \lambda^*\left(\gamma^*\right)^2\chi_2\left(Q_0\|Q_1\right)}}. \quad (4.55)$$

Proof. Consider a capacity-achieving codebook $\mathcal{C}^*$ for the channel between Alice and Willie. For a fixed common message $W_2 = j$, consider a sequence of covert communication schemes characterized by $\epsilon_{n,j} \triangleq \mathbb{P}\Big(\widehat{W_1} \neq W_1 | W_2 = j\Big)$, $\delta_{n,j} \triangleq \mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big)$, and $\log M_1$ takes the maximum value such that $\lim_{n\to\infty} \log M_1 = \infty$. Note that $\lim_{n\to\infty} \epsilon_{n,j} = \lim_{n\to\infty} \delta_{n,j} = 0$ since $\lim_{n\to\infty} \epsilon_n = \lim_{n\to\infty} \delta_n = 0$. We denote the innocent codeword corresponding to $W_2 = j$ by $\mathbf{x}_{0j} = (x_{0j,1}, x_{0j,2}, \ldots, x_{0j,n}) \in \mathcal{C}^*$, the innocent symbol at position ℓ by $x_{0j,\ell}$, and the information symbol at position ℓ by $x_{0j,\ell}^c \triangleq 1 - x_{0j,\ell}$. For a fixed $W_2 = j$, Alice transmits an n-length codeword $\mathbf{X}_{ij} = (X_{ij,1}, X_{ij,2}, \ldots, X_{ij,n})$, $i \in [\![1, M_1]\!]$, and we denote the distribution of the codeword by Π_j^n and the distribution of the symbol at position ℓ by $\Pi_{j,\ell}$, where

$$\Pi_{j,\ell}(x) \triangleq \frac{1}{M_1}\sum_{i=1}^{M_1} \mathbb{1}\{X_{ij,\ell} = x\}. \quad (4.56)$$

We define $\Pi_{j,\ell}(x_{0j,\ell}^c) = 1 - \Pi_{j,\ell}(x_{0j,\ell}) = \mu_{j,\ell}^{(n)}$. We interpret $\mu_{j,\ell}^{(n)}$ as the probability of flipping innocent symbol $x_{0j,\ell}$ to information symbol $x_{0j,\ell}^c$ at symbol position $\ell \in [\![1, n]\!]$. Note that the innocent symbol $x_{0j,\ell}$ depends on the choice of the common message $W_2 = j$ and the symbol position ℓ. For $W_2 = j$ and every $n \in \mathbb{N}^*$, we define a permutation $\pi_j^{(n)}$ of $[\![1, n]\!]$ to define a new code such that

$$\mu_{j,1}^{(n)} = \max_{\ell\in[\![1,n]\!]} \mu_{j,\ell}^{(n)}. \quad (4.57)$$

The performance of the new code that satisfies (4.57) is identical to that of the original

code since the channel is memoryless. Hence, without loss of generality, we only study the sequence of codes that satisfies (4.57) for every $n \in \mathbb{N}^*$. For conciseness, we define the following terms.

$$P^0_{j,\ell}(y) \triangleq W_{Y|X}(y|x_{0j,\ell}), \quad P^1_{j,\ell}(y) \triangleq W_{Y|X}(y|x^c_{0j,\ell}), \tag{4.58}$$

$$Q^0_{j,\ell}(z) \triangleq W_{Z|X}(z|x_{0j,\ell}), \quad Q^1_{j,\ell}(z) \triangleq W_{Z|X}(z|x^c_{0j,\ell}). \tag{4.59}$$

Define $K_{j,\ell}(z) \triangleq Q^1_{j,\ell}(z) - Q^0_{j,\ell}(z)$. Note that $\forall z \in \mathcal{Z}$, $K_{j,\ell}(z)$ equals either $Q_1(z) - Q_0(z)$ or $Q_0(z) - Q_1(z)$ depending on the choices of j and ℓ. Defining $K(z) \triangleq |K_{j,\ell}(z)|$, we remove the dependency of $K(z)$ on j and ℓ. We define the distribution of each symbol Z_ℓ of $\mathbf{Z}$ by $\widehat{Q}_{j,\ell}$, where

$$\widehat{Q}_{j,\ell}(z) \triangleq \sum_x \Pi_{j,\ell}(x) W_{Z|X}(z|x) \tag{4.60}$$

$$= Q^0_{j,\ell}(z) + \mu^{(n)}_{j,\ell} K_{j,\ell}(z). \tag{4.61}$$

Let us now analyze the KL divergence between $\widehat{Q}^n_j$ and $\overline{Q}^n_j$.

$$\delta_{n,j} = \sum_{\mathbf{z}} \widehat{Q}^n_j(\mathbf{z}) \log \frac{\widehat{Q}^n_j(\mathbf{z})}{\overline{Q}^n_j(\mathbf{z})} \tag{4.62}$$

$$= -\mathbb{H}(\mathbf{Z}|W_2 = j) - \sum_{\mathbf{z}} \widehat{Q}^n_j(\mathbf{z}) \log \overline{Q}^n_j(\mathbf{z}) \tag{4.63}$$

$$= \sum_{\ell=1}^{n} \left(-\mathbb{H}\big(Z_\ell | \mathbf{Z}_1^{\ell-1}, W_2 = j\big) - \sum_z \widehat{Q}_{j,\ell}(z) \log Q^0_{j,\ell}(z) \right) \tag{4.64}$$

$$\geqslant \sum_{\ell=1}^{n} \left(-\mathbb{H}(Z_\ell|W_2 = j) - \sum_z \widehat{Q}_{j,\ell(z)} \log Q^0_{j,\ell}(z) \right) \tag{4.65}$$

$$= \sum_{\ell=1}^{n} \mathbb{D}\Big(\widehat{Q}_{j,\ell} \| Q^0_{j,\ell} \Big) \tag{4.66}$$

Since $\delta_{n,j}$ vanishes in the limit of large blocklength and since KL divergence is non-negative, we have $\lim_{n\to\infty} \mathbb{D}\Big(\widehat{Q}_{j,1} \| Q^0_{j,1} \Big) = 0$. Using Pinsker's inequality, we obtain

$\lim_{n\to\infty} \mathbb{V}\Big(\widehat{Q}_{j,1}, Q^0_{j,1}\Big) = 0$, which implies that $\forall z \in \mathcal{Z}$,

$$\lim_{n\to\infty} \left|\widehat{Q}_{j,1}(z) - Q^0_{j,1}(z)\right| = 0, \tag{4.67}$$

$$\lim_{n\to\infty} \mu^{(n)}_{j,1} K(z) = 0. \tag{4.68}$$

However, $K(z)$ is not exactly zero for all $z \in \mathcal{Z}$, since $Q_1 \neq Q_0$. Hence, we obtain $\lim_{n\to\infty} \mu^{(n)}_{j,1} = 0$. Consequently, from (4.57), we conclude that $\lim_{n\to\infty} \mu^{(n)}_{j,\ell} = 0$ for all $\ell \in [\![1, n]\!]$. Next, define

$$\Psi^{(n)}_{j,\ell}(z) \triangleq \mu^{(n)}_{j,\ell} K_{j,\ell}(z), \tag{4.69}$$

$$\xi^{(n)}_{j,\ell}(z) \triangleq \frac{\Psi^{(n)}_{j,\ell}(z)}{Q^0_{j,\ell}(z)} + \frac{4}{3}\frac{\left|\Psi^{(n)}_{j,\ell}(z)\right|}{Q^0_{j,\ell}(z)}, \tag{4.70}$$

$$\xi^{(n)}_{j}(z) \triangleq \max_{\ell\in[\![1,n]\!]} \xi^{(n)}_{j,\ell}(z). \tag{4.71}$$

Since $\lim_{n\to\infty} \mu^{(n)}_{j,\ell} = 0$, we have $\lim_{n\to\infty} \Psi^{(n)}_{j,\ell}(z) = \lim_{n\to\infty} \xi^{(n)}_{j,\ell}(z) = 0$ for all $z \in \mathcal{Z}$ and $\ell \in [\![1, n]\!]$. We bound $\xi^{(n)}_j(z)$ defined in (4.71) by

$$\xi^{(n)}_j(z) \leqslant \frac{\left|\Psi^{(n)}_{j,\ell}(z)\right|}{Q^0_{j,\ell}(z)} + \frac{4}{3}\frac{\left|\Psi^{(n)}_{j,\ell}(z)\right|}{Q^0_{j,\ell}(z)} \tag{4.72}$$

$$= \frac{7}{3}\frac{\left|\Psi^{(n)}_{j,\ell}(z)\right|}{Q^0_{j,\ell}(z)} \tag{4.73}$$

$$\leqslant \frac{7}{3}\frac{\mu^{(n)}_{j,1} K(z)}{Q^0_{j,\ell}(z)}. \tag{4.74}$$

Combining (4.74) and the fact that $\xi^{(n)}_j(z)$ is non-negative by definition, we conclude that $\lim_{n\to\infty} \xi^{(n)}_j(z) = 0$, $\forall z \in \mathcal{Z}$. Continuing the analysis of $\delta_{n,j}$ from (4.66), we

have, for n large enough,

$$\delta_{n,j} \geqslant \sum_{\ell=1}^{n} \sum_{z} \widehat{Q}_{j,\ell}(z) \log \left(1 + \frac{\mu_{j,\ell}^{(n)} K_{j,\ell}(z)}{Q_{j,\ell}^{0}(z)} \right) \tag{4.75}$$

$$\overset{(a)}{\geqslant} \sum_{\ell=1}^{n} \sum_{z} \frac{\left(\Psi_{j,\ell}^{(n)}(z) \right)^2}{2Q_{j,\ell}^{0}(z)} \left(1 - \frac{\Psi_{j,\ell}^{(n)}(z)}{Q_{j,\ell}^{0}(z)} - \frac{4 \left| \Psi_{j,\ell}^{(n)}(z) \right|}{3Q_{j,\ell}^{0}(z)} \right) \tag{4.76}$$

$$= \sum_{\ell=1}^{n} \sum_{z} \frac{\left(\Psi_{j,\ell}^{(n)}(z) \right)^2}{2Q_{j,\ell}^{0}(z)} \left(1 - \xi_{j,\ell}^{(n)}(z) \right) \tag{4.77}$$

$$\geqslant \sum_{z} \left(1 - \xi_{j}^{(n)}(z) \right) \sum_{\ell=1}^{n} \frac{\left(\Psi_{j,\ell}^{(n)}(z) \right)^2}{2Q_{j,\ell}^{0}(z)}, \tag{4.78}$$

where (a) follows from the fact that $\log(1+x) \geqslant x - \frac{x^2}{2}$, for $x \geqslant 0$, $\log(1+x) \geqslant x - \frac{x^2}{2} + \frac{2x^3}{3}$, for $x \in \left[-\frac{1}{2}, 0\right]$, and $\sum_z \Psi_{j,\ell}^{(n)} = 0$. Then, we define

$$n_{j,1} \triangleq \mathrm{wt}\left(\mathbf{x}_{0j}\right), \quad n_{j,0} \triangleq n - n_{j,1}, \tag{4.79}$$

$$\rho_{j,0}^{(n)} \triangleq \frac{\sum_{\ell:x_{0j,\ell}=0}^{n \ell=1} \mu_{j,\ell}^{(n)}}{n_{j,0}}, \quad \rho_{j,1}^{(n)} \triangleq \frac{\sum_{\ell:x_{0j,\ell}=1}^{n \ell=1} \mu_{j,\ell}^{(n)}}{n_{j,1}}, \tag{4.80}$$

$$\gamma_{j}^{(n)} \triangleq \frac{\rho_{j,1}^{(n)}}{\rho_{j,0}^{(n)}}, \quad \lambda_{j}^{(n)} \triangleq \frac{n_{j,1}}{n}, \tag{4.81}$$

where $n_{j,0}$ and $n_{j,1}$ denote the number of 0's and 1's in $\mathbf{x}_{0j}$, respectively; $\rho_{j,0}^{(n)}$ and $\rho_{j,1}^{(n)}$ are the average flipping probabilities from 0 to 1 and from 1 to 0, respectively. Note that $\lim_{n\to\infty} \rho_{j,0}^{(n)} = 0$ and $\lim_{n\to\infty} \rho_{j,1}^{(n)} = 0$. In addition, we set $\lim_{n\to\infty} \gamma_{j}^{(n)} = \gamma_{j}^{\dagger} \in \mathbb{R}^{+}$. If $\lim_{n\to\infty} \gamma_{j}^{(n)} = 0$ or ∞, only symbols in positions either with innocent symbol 0 or 1, respectively, are used to embed covert information. Else, the sequence $\{\gamma_{j}^{(n)}\}$ is bounded, and we can extract a convergent subsequence $\{\gamma_{j}^{(n)}\}_{n\in\mathcal{N}}$, where $\mathcal{N} \subseteq \mathbb{N}^{*}$ is an infinite set, with limit $\gamma_{j}^{\dagger}$. Henceforth, we only consider the subsequence of codes with blocklength $n \in \mathcal{N}$. Note that $1 - \lambda_{j}^{(n)} = \frac{n_{j,0}}{n}$. Using Cauchy-Schwarz inequality,

we obtain

$$\sum_{\substack{\ell=1\\ \ell:x_{0j,\ell}=0}}^{n} \left(\mu_{j,\ell}^{(n)}\right)^2 \geqslant \frac{1}{n_{j,0}} \left(\sum_{\substack{\ell=1\\ \ell:x_{0j,\ell}=0}}^{n} \mu_{j,\ell}^{(n)} \right)^2, \tag{4.82}$$

$$\sum_{\substack{\ell=1\\ \ell:x_{0j,\ell}=1}}^{n} \left(\mu_{j,\ell}^{(n)}\right)^2 \geqslant \frac{1}{n_{j,1}} \left(\sum_{\substack{\ell=1\\ \ell:x_{0j,\ell}=1}}^{n} \mu_{j,\ell}^{(n)} \right)^2. \tag{4.83}$$

From (4.78), we continue to bound $\delta_{n,j}$ by

$$\delta_{n,j} \geqslant \sum_z \frac{1}{2}\left(1-\xi_j^{(n)}(z)\right) \left(\sum_{\substack{\ell=1\\ \ell:x_{0j,\ell}=0}}^{n} \left(\mu_{j,\ell}^{(n)}\right)^2 \frac{K^2(z)}{Q_0(z)} + \sum_{\substack{\ell=1\\ \ell:x_{0j,\ell}=1}}^{n} \left(\mu_{j,\ell}^{(n)}\right)^2 \frac{K^2(z)}{Q_1(z)} \right) \tag{4.84}$$

$$\overset{(a)}{\geqslant} \sum_z \frac{1}{2}\left(1-\xi_j^{(n)}(z)\right) \times \left(\frac{1}{n_{j,0}} \left(\sum_{\substack{\ell=1\\ \ell:x_{0j,\ell}=0}}^{n} \mu_{j,\ell}^{(n)} \right)^2 \frac{K^2(z)}{Q_0(z)} + \frac{1}{n_{j,1}} \left(\sum_{\substack{\ell=1\\ \ell:x_{0j,\ell}=1}}^{n} \mu_{j,\ell}^{(n)} \right)^2 \frac{K^2(z)}{Q_1(z)} \right) \tag{4.85}$$

$$= \sum_z \frac{1}{2}\left(1-\xi_j^{(n)}(z)\right) \left(n_{j,0}\left(\rho_{j,0}^{(n)}\right)^2 \frac{K^2(z)}{Q_0(z)} + n_{j,1}\left(\rho_{j,1}^{(n)}\right)^2 \frac{K^2(z)}{Q_1(z)} \right) \tag{4.86}$$

$$= \sum_z \frac{1}{2} n \left(\rho_{j,0}^{(n)}\right)^2 \left(1-\xi_j^{(n)}(z)\right) \left((1-\lambda_j^{(n)}) \frac{K^2(z)}{Q_0(z)} + \lambda_j^{(n)} \left(\gamma_j^{(n)}\right)^2 \frac{K^2(z)}{Q_1(z)} \right), \tag{4.87}$$

where (a) follows from (4.82) and (4.83).

We pause the analysis of $\delta_{n,j}$ here and define constant composition sub-codebooks [82] $\mathcal{F}_k \subset \mathcal{C}^*$ with type P_k in which k denotes the weight of any codeword of that type. As there are $(n+1)$ different types for sequences $\{0,1\}^n$, there are at most $(n+1)$ such sub-codebooks. Let us recall that the codebook $\mathcal{C}^*$ is a capacity-achieving codebook for the channel between Alice and Willie; that is, the rate of the common

message $R \triangleq \frac{\log M_2}{n} = \mathbb{I}\left(\Lambda, W_{Z|X}\right) - \delta(n)$ with $\lim_{n\to\infty} \delta(n) = 0$. Let us assume that $\forall k \in [\![1, n]\!]$, $\frac{\log|\mathcal{F}_k|}{n} \leqslant R - \delta$ for any $\delta > 0$. For a $\delta' < \delta$ and n large enough,

$$M_2 = \sum_k |\mathcal{F}_k| \tag{4.88}$$

$$\leqslant \sum_k \exp\left(n\left(R - \delta\right)\right) \tag{4.89}$$

$$= (n+1)\exp\left(n\left(R - \delta\right)\right) \tag{4.90}$$

$$\leqslant \exp\left(n\left(R - \delta'\right)\right). \tag{4.91}$$

We note that the assumption $\frac{\log|\mathcal{F}_k|}{n} \leqslant R - \delta$ for all $k \in [\![1, n]\!]$ results in a contradiction in (4.91) since $M_2 = \exp(nR)$. Hence, there exists at least one sub-codebook $\mathcal{F}_{k^*}$ such that

$$\frac{\log|\mathcal{F}_{k^*}|}{n} > R - \delta \tag{4.92}$$

and $P_{k^*}(1) = 1 - P_{k^*}(0) = \frac{k^*}{n} \in (0, 1)$. Using [82, Corollary 6.4], we bound the rate of this sub-codebook for an arbitrary $\upsilon > 0$ by

$$\frac{\log|\mathcal{F}_{k^*}|}{n} < \mathbb{I}\left(P_{k^*}, W_{Z|X}\right) + 2\upsilon. \tag{4.93}$$

Combining (4.92) and (4.93), we obtain

$$\mathbb{I}\left(P_{k^*}, W_{Z|X}\right) > \mathbb{I}\left(\Lambda, W_{Z|X}\right) - \delta - 2\upsilon. \tag{4.94}$$

Using the unicity of the capacity-achieving input distribution, the concavity of mutual information and (4.94), we conclude that the type P_{k^*} is arbitrarily close to Λ since δ and υ are arbitrary. Consequently, we replace $\lambda_j^{(n)}$ with $\lambda^\dagger \triangleq \lambda^* - \epsilon$ for an arbitrarily small $\epsilon \in \mathbb{R}$.

We then bound $\log M_1$ using standard converse steps.

$$\log M_1 = \mathbb{H}(W_1|W_2 = j) \tag{4.95}$$

$$\leqslant \mathbb{I}(W_1; \mathbf{Y}|W_2 = j) + \mathbb{H}_b\left(\epsilon_{n,j}\right) + \epsilon_{n,j} \log M_1 \tag{4.96}$$

$$\leqslant \mathbb{I}(W_1\mathbf{X}; \mathbf{Y}|W_2 = j) + \mathbb{H}_b\left(\epsilon_{n,j}\right) + \epsilon_{n,j} \log M_1 \tag{4.97}$$

$$= \mathbb{I}(\mathbf{X}; \mathbf{Y}|W_2 = j) + \mathbb{I}(W_1; \mathbf{Y}|W_2 = j, \mathbf{X}) + \mathbb{H}_b\left(\epsilon_{n,j}\right) + \epsilon_{n,j} \log M_1 \tag{4.98}$$

$$\overset{(a)}{=} \mathbb{H}(\mathbf{Y}|W_2 = j) - \mathbb{H}(\mathbf{Y}|\mathbf{X}, W_2 = j) + \mathbb{H}_b\left(\epsilon_{n,j}\right) + \epsilon_{n,j} \log M_1 \tag{4.99}$$

$$\overset{(b)}{\leqslant} \sum_{\ell=1}^{n} \left(\mathbb{H}(Y_\ell|W_2 = j) - \mathbb{H}(Y_\ell|X_\ell, W_2 = j)\right) + \mathbb{H}_b\left(\epsilon_{n,j}\right) + \epsilon_{n,j} \log M_1 \tag{4.100}$$

$$= \sum_{\ell=1}^{n} \mathbb{I}(X_\ell; Y_\ell|W_2 = j) + \mathbb{H}_b\left(\epsilon_{n,j}\right) + \epsilon_{n,j} \log M_1, \tag{4.101}$$

where (a) follows from the fact that $\mathbb{I}(W_1; \mathbf{Y}|W_2 = j, \mathbf{X}) = 0$, and (b) follows from the fact that conditioning reduces entropy and the memoryless property of the channel $W_{Y|X}$. Rearranging the terms in (4.101), we obtain

$$\log M_1 \leqslant \frac{\sum_{\ell=1}^{n} \mathbb{I}(X_\ell; Y_\ell|W_2 = j) + \mathbb{H}_b\left(\epsilon_{n,j}\right)}{1 - \epsilon_{n,j}}. \tag{4.102}$$

Defining $\widehat{P}_{j,\ell}$ as the distribution of symbol Y_ℓ of $\mathbf{Y}$, we upper bound the mutual information term in (4.102) by

$$\mathbb{I}(X_\ell; Y_\ell|W_2 = j)$$

$$= \sum_{y} \left(\left(1 - \mu_{j,\ell}^{(n)}\right) P_{j,\ell}^{0}(y) \log \frac{P_{j,\ell}^{0}(y)}{\widehat{P}_{j,\ell}(y)} \right) + \sum_{y} \left(\left(\mu_{j,\ell}^{(n)}\right) P_{j,\ell}^{1}(y) \log \frac{P_{j,\ell}^{1}(y)}{\widehat{P}_{j,\ell}(y)} \right) \tag{4.103}$$

$$= \mu_{j,\ell}^{(n)} \mathbb{D}\big(P_{j,\ell}^{1} \| P_{j,\ell}^{0}\big) - \mathbb{D}\Big(\widehat{P}_{j,\ell} \| P_{j,\ell}^{0}\Big) \tag{4.104}$$

$$\leqslant \mu_{j,\ell}^{(n)} \mathbb{D}\big(P_{j,\ell}^{1} \| P_{j,\ell}^{0}\big). \tag{4.105}$$

Combining (4.102) and (4.105), we obtain

$$\log M_1 \leqslant \frac{\sum_{\ell=1}^{n} \mu_{j,\ell}^{(n)} \mathbb{D}\big(P_{j,\ell}^{1} \| P_{j,\ell}^{0}\big) + \mathbb{H}_b\left(\epsilon_{n,j}\right)}{1-\epsilon_{n,j}} \tag{4.106}$$

$$= \frac{n_{j,0}\rho_{j,0}^{(n)} \mathbb{D}(P_1\|P_0) + n_{j,1}\rho_{j,1}^{(n)} \mathbb{D}(P_0\|P_1) + \mathbb{H}_b\left(\epsilon_{n,j}\right)}{1-\epsilon_{n,j}} \tag{4.107}$$

$$= \frac{n\rho_{j,0}^{(n)} \Big((1-\lambda^{\dagger}) \mathbb{D}(P_1\|P_0) + \lambda^{\dagger}\gamma_j^{(n)} \mathbb{D}(P_0\|P_1)\Big) + \mathbb{H}_b\left(\epsilon_{n,j}\right)}{1-\epsilon_{n,j}}. \tag{4.108}$$

Since $\lim_{\substack{n\to\infty \\ n\in\mathcal{N}}} \log M_1 = \infty$, (4.108) implies that $\lim_{\substack{n\to\infty \\ n\in\mathcal{N}}} n\rho_{j,0}^{(n)} = \infty$. Consequently, from (4.87), we conclude that $\lim_{\substack{n\to\infty \\ n\in\mathcal{N}}} \sqrt{n\delta_{n,j}} = \infty$. Combining (4.87), (4.108), and the facts that $\lim_{\substack{n\to\infty \\ n\in\mathcal{N}}} \sqrt{n\delta_{n,j}} = \infty$ and $\lim_{\substack{n\to\infty \\ n\in\mathcal{N}}} \mathbb{H}_b\left(\epsilon_{n,j}\right) = 0$, we obtain

$$\begin{aligned}
&\liminf_{\substack{n\to\infty \\ n\in\mathcal{N}}} \frac{\log M_1}{\sqrt{n\delta_{n,j}}} \\
&\leqslant \liminf_{\substack{n\to\infty \\ n\in\mathcal{N}}} \frac{n\rho_{j,0}^{(n)} \Big((1-\lambda^{\dagger}) \mathbb{D}(P_1\|P_0) + \lambda^{\dagger}\gamma_j^{(n)} \mathbb{D}(P_0\|P_1)\Big)}{(1-\epsilon_{n,j}) \sqrt{n \sum_z \frac{n\left(\rho_{j,0}^{(n)}\right)^2}{2} \left(1-\xi_j^{(n)}(z)\right) \left((1-\lambda^{\dagger}) \frac{K^2(z)}{Q_0(z)} + \lambda^{\dagger} \left(\gamma_j^{(n)}\right)^2 \frac{K^2(z)}{Q_1(z)}\right)}}
\end{aligned} \tag{4.109}$$

$$= \sqrt{2} \frac{(1-\lambda^{\dagger}) \mathbb{D}(P_1\|P_0) + \lambda^{\dagger}\gamma_j^{\dagger} \mathbb{D}(P_0\|P_1)}{\sqrt{(1-\lambda^{\dagger})\, \chi_2\left(Q_1\|Q_0\right) + \lambda^{\dagger} \left(\gamma_j^{\dagger}\right)^2 \chi_2\left(Q_0\|Q_1\right)}}. \tag{4.110}$$

Following standard steps, we lower bound $\log M_1$ by

$$\log M_1 = \mathbb{H}(W_1|W_2=j) \tag{4.111}$$

$$\geqslant \mathbb{I}(W_1; \mathbf{Z}|W_2=j) \tag{4.112}$$

$$\overset{(a)}{=} \mathbb{H}(\mathbf{Z}|W_2=j) - \mathbb{H}(\mathbf{Z}|\mathbf{X}, W_1, W_2=j) \tag{4.113}$$

$$\overset{(b)}{\geqslant} \mathbb{H}(\mathbf{Z}|W_2=j) - \mathbb{H}(\mathbf{Z}|\mathbf{X}, W_2=j) \tag{4.114}$$

$$= \sum_{\mathbf{x}} \sum_{\mathbf{z}} \Pi_j^n(\mathbf{x}) W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{x}) \log \frac{W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{x})}{\widehat{Q}_j^n(\mathbf{z})} \tag{4.115}$$

$$= \sum_{\ell=1}^{n} \sum_{x} \sum_{z} \Pi_{j,\ell}(x) W_{Z|X}(z|x) \log \frac{W_{Z|X}(z|x)}{Q^0_{j,\ell}(z)} - \delta_{n,j} \tag{4.116}$$

$$\overset{(c)}{\geqslant} \sum_{\ell=1}^{n} \mathbb{I}(X_\ell; Z_\ell | W_2 = j) - \delta_{n,j}, \tag{4.117}$$

where (a) follows from the fact that $\mathbf{X}$ is a function of (W_1, W_2), (b) follows from the fact that conditioning reduces entropy, and (c) follows from (4.60) and the fact that KL divergence is non-negative. Continuing the analysis of $\log M_1$ by expanding the mutual information term, we obtain

$$\log M_1 \geqslant \sum_{\ell=1}^{n} \sum_{z} \left(1 - \mu^{(n)}_{j,\ell}\right) Q^0_{j,\ell}(z) \log \frac{Q^0_{j,\ell}(z)}{\widehat{Q}_{j,\ell}(z)} + \sum_{\ell=1}^{n} \sum_{z} \left(\mu^{(n)}_{j,\ell}\right) Q^1_{j,\ell}(z) \log \frac{Q^1_{j,\ell}(z)}{\widehat{Q}_{j,\ell}(z)} - \delta_{n,j} \tag{4.118}$$

$$\geqslant \sum_{\ell=1}^{n} \mu^{(n)}_{j,\ell} \mathbb{D}\big(Q^1_{j,\ell} \| Q^0_{j,\ell}\big) - \sum_{\ell=1}^{n} \mathbb{D}\Big(\widehat{Q}_{j,\ell} \| Q^0_{j,\ell}\Big) - \delta_{n,j} \tag{4.119}$$

$$\overset{(a)}{\geqslant} \sum_{\ell=1}^{n} \mu^{(n)}_{j,\ell} \mathbb{D}\big(Q^1_{j,\ell} \| Q^0_{j,\ell}\big) - 2\delta_{n,j} \tag{4.120}$$

$$= n\rho^{(n)}_{j,0} \Big((1-\lambda^\dagger) \mathbb{D}(Q_1 \| Q_0) + \lambda^\dagger \gamma^{(n)}_j \mathbb{D}(Q_0 \| Q_1) \Big) - 2\delta_{n,j}, \tag{4.121}$$

where (a) follows from (4.66). For an arbitrary $\nu \in (0,1)$, an n large enough, and for a subsequence of codes that achieves[4] the right hand side of (4.110), we have

$$\liminf_{\substack{n\to\infty \\ n\in\mathcal{N}}} \frac{\log M_1}{\sqrt{n\delta_{n,j}}} \geqslant (1-\nu)\sqrt{2} \frac{(1-\lambda^\dagger)\mathbb{D}(P_1\|P_0) + \lambda^\dagger \gamma^\dagger_j \mathbb{D}(P_0\|P_1)}{\sqrt{(1-\lambda^\dagger)\,\chi_2\left(Q_1\|Q_0\right) + \lambda^\dagger \left(\gamma^\dagger_j\right)^2 \chi_2\left(Q_0\|Q_1\right)}}. \tag{4.122}$$

[4]We know that there exists at least one such code from Theorem 3.

For that sequence of codes, using (4.108), we obtain

$$\liminf_{\substack{n\to\infty \\ n\in\mathcal{N}}} \frac{n\rho_{j,0}^{(n)}\left((1-\lambda^\dagger)\mathbb{D}(P_1\|P_0)+\lambda^\dagger\gamma_j^{(n)}\mathbb{D}(P_0\|P_1)\right)}{\sqrt{n\delta_{n,j}}\,(1-\epsilon_{n,j})} \geqslant \frac{(1-\nu)\sqrt{2}\left((1-\lambda^\dagger)\mathbb{D}(P_1\|P_0)+\lambda^\dagger\gamma_j^\dagger\mathbb{D}(P_0\|P_1)\right)}{\sqrt{(1-\lambda^\dagger)\,\chi_2\left(Q_1\|Q_0\right)+\lambda^\dagger\left(\gamma_j^\dagger\right)^2\chi_2\left(Q_0\|Q_1\right)}}. \quad (4.123)$$

On further simplifying (4.123), we obtain

$$\liminf_{\substack{n\to\infty \\ n\in\mathcal{N}}} \frac{n\rho_{j,0}^{(n)}}{\sqrt{n\delta_{n,j}}} \geqslant \frac{(1-\nu)\sqrt{2}}{\sqrt{(1-\lambda^\dagger)\,\chi_2\left(Q_1\|Q_0\right)+\lambda^\dagger\left(\gamma_j^\dagger\right)^2\chi_2\left(Q_0\|Q_1\right)}}. \quad (4.124)$$

Since $\limsup_{n\to\infty} a_n \geqslant \liminf_{n\to\infty} a_n$ for any sequence $\{a_n\}$, we have

$$\limsup_{\substack{n\to\infty \\ n\in\mathcal{N}}} \frac{n\rho_{j,0}^{(n)}}{\sqrt{n\delta_{n,j}}} \geqslant \frac{(1-\nu)\sqrt{2}}{\sqrt{(1-\lambda^\dagger)\,\chi_2\left(Q_1\|Q_0\right)+\lambda^\dagger\left(\gamma_j^\dagger\right)^2\chi_2\left(Q_0\|Q_1\right)}}. \quad (4.125)$$

Combining (4.121) and (4.125) and letting $\epsilon \downarrow 0$ in the definition of $\lambda^\dagger$ and $\nu \downarrow 0$ in (4.125), we obtain

$$\limsup_{\substack{n\to\infty \\ n\in\mathcal{N}}} \frac{\log M_1}{\sqrt{n\delta_{n,j}}} \geqslant \frac{\sqrt{2}\left((1-\lambda^*)\mathbb{D}(Q_1\|Q_0)+\lambda^*\gamma_j^\dagger\mathbb{D}(Q_0\|Q_1)\right)}{\sqrt{(1-\lambda^*)\chi_2\left(Q_1\|Q_0\right)+\lambda^*\left(\gamma_j^\dagger\right)^2\chi_2\left(Q_0\|Q_1\right)}}. \quad (4.126)$$

Note that the bounds (4.110) and (4.126) still depend on the choice of the common message $W_2 = j$ through $\gamma_j^\dagger$. To eliminate this dependency, we choose an optimal $\gamma^* \geqslant 0$ that maximizes the right hand side of (4.110) provided the following condition is satisfied.

$$(1-\lambda^*)\mathbb{D}(P_1\|P_0)+\lambda^*\gamma^*\mathbb{D}(P_0\|P_1) \geqslant (1-\lambda^*)\mathbb{D}(Q_1\|Q_0)+\lambda^*\gamma^*\mathbb{D}(Q_0\|Q_1). \quad (4.127)$$

Consequently, replacing $\gamma_j^\dagger$ with γ^* in (4.110) and (4.126), we obtain (4.54) and (4.55).

□

For the subsequence of codes with blocklength $n \in \mathcal{N}$, where $\mathcal{N} \subseteq \mathbb{N}^*$ is an infinite set, that achieves the right hand side of (4.54), we have

$$\limsup_{\substack{n\to\infty \\ n\in\mathcal{N}}} \frac{\log M_1}{\sqrt{n\mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big)}} = \sqrt{2}\frac{(1-\lambda^*)\,\mathbb{D}(P_1\|P_0) + \lambda^*\gamma^*\mathbb{D}(P_0\|P_1)}{\sqrt{(1-\lambda^*)\,\chi_2\left(Q_1\|Q_0\right) + \lambda^*\left(\gamma^*\right)^2\chi_2\left(Q_0\|Q_1\right)}}, \quad (4.128)$$

for some γ^* that achieves the maximum in (4.54). According to Theorem 4, for that subsequence of codes, $\limsup_{\substack{n\to\infty \\ n\in\mathcal{N}}} \frac{\log M_1}{\sqrt{n\mathbb{D}\left(\widehat{Q}_j^n \| \overline{Q}_j^n\right)}}$ is lower bounded as in (4.55). The combination of (4.55) and (4.128) imposes

$$(1-\lambda^*)\,\mathbb{D}(P_1\|P_0) + \lambda^*\gamma\mathbb{D}(P_0\|P_1) \geqslant (1-\lambda^*)\,\mathbb{D}(Q_1\|Q_0) + \lambda^*\gamma\mathbb{D}(Q_0\|Q_1), \quad (4.129)$$

which characterizes the advantage that Bob should possess over Willie to facilitate keyless embedding of covert bits. Although we normalize $\log M_1$ by $\sqrt{n\mathbb{D}\Big(\widehat{Q}_j^n \| \overline{Q}_j^n\Big)}$, which depends on the choice of the common message $W_2 = j$, the bounds on $\log M_1$ are independent of j.

Also, for any sequence $\{a_n\}_{n\in\mathbb{N}^*}$ and any infinite set $\mathcal{N} \subseteq \mathbb{N}^*$, we have $\liminf_{n\to\infty} a_n \leqslant \liminf_{\substack{n\to\infty \\ n\in\mathcal{N}}} a_n$ and $\limsup_{n\to\infty} a_n \geqslant \limsup_{\substack{n\to\infty \\ n\in\mathcal{N}}} a_n$. Combining this fact with Theorem 3 and Theorem 4, we conclude that the optimal covert embedding throughput when the common message is transmitted at a rate close to the capacity of the channel to Willie, is given by

$$\sqrt{2}\frac{(1-\lambda^*)\,\mathbb{D}(P_1\|P_0) + \lambda^*\gamma^*\mathbb{D}(P_0\|P_1)}{\sqrt{(1-\lambda^*)\,\chi_2\left(Q_1\|Q_0\right) + \lambda^*\left(\gamma^*\right)^2\chi_2\left(Q_0\|Q_1\right)}}, \quad (4.130)$$

where $\gamma^* \geqslant 0$ is the largest number that satisfies (4.129).

In our main result, λ^* is related to the unique capacity-achieving input distribution

for the channel to Willie. In a sense, λ^* denotes the fraction of symbol positions in which symbol 1 serves as the innocent symbol; subsequently, $(1-\lambda^*)$ denotes the fraction of symbol positions in which symbol 0 is the innocent symbol. Note that in (4.17), all terms except γ are fixed by the channel. γ is a parameter that can be tuned at the transmitter, and it corresponds to the ratio of the probability of flipping 1 to 0 to the probability of flipping 0 to 1. Setting γ to 0 or ∞ results in the extreme case of using only one of the symbols to embed information.

Remark 1. *As a special case, let us assume that the channel to Willie is degraded w.r.t. the channel to Bob. This assumption guarantees that* (4.129) *is satisfied as degradedness implies* $\mathbb{D}(P_1\|P_0) > \mathbb{D}(Q_1\|Q_0)$ *and* $\mathbb{D}(P_0\|P_1) > \mathbb{D}(Q_0\|Q_1)$. *Hence, in this case, covert information can be embedded on top of innocent transmissions. However, the degraded broadcast channel assumption is not a necessary condition to facilitate keyless covert communication in our case. As an example, let us consider a discrete memoryless channel* $\left(\mathcal{X}, W_{Z|X}, \mathcal{Z}\right)$ *with* $\mathbb{D}(P_1\|P_0) < \mathbb{D}(Q_1\|Q_0)$ *and* $\mathbb{D}(P_0\|P_1) > \mathbb{D}(Q_0\|Q_1)$. *Here, the channel* $W_{Z|X}$ *is not degraded w.r.t. the channel* $W_{Y|X}$. *Since all KL divergence terms and* λ^* *in* (4.129) *are determined by the channel, the only degree of freedom is* γ. *By choosing a* γ *that satisfies* (4.129), *covert information can be transmitted by embedding it on top of innocent transmissions without using a secret key despite the channel to Willie not being degraded w.r.t. the channel to Bob.*

Remark 2. *For symmetric channels with two inputs, note that* $\mathbb{D}(P_1\|P_0) = \mathbb{D}(P_0\|P_1)$, $\mathbb{D}(Q_1\|Q_0) = \mathbb{D}(Q_0\|Q_1)$, *and* $\chi_2\left(Q_1\|Q_0\right) = \chi_2\left(Q_0\|Q_1\right)$. *Consequently, from* (4.54), *we obtain*

$$\liminf_{n\to\infty} \frac{\log M_1}{\sqrt{n\mathbb{D}\left(\widehat{Q}_j^n \| \overline{Q}_j^n\right)}} \leqslant \sqrt{2}\frac{\mathbb{D}(P_1\|P_0)}{\sqrt{\chi_2\left(Q_1\|Q_0\right)}}, \tag{4.131}$$

since $\gamma^* = 1$ *and* $\lambda^* = \frac{1}{2}$. *For the subsequece of codes that achieves the right hand side of* (4.131)*, we obtain from* (4.55)*,*

$$\limsup_{n\to\infty} \frac{\log M_1}{\sqrt{n\mathbb{D}\left(\widehat{Q}_j^n \| \overline{Q}_j^n\right)}} \geqslant \sqrt{2} \frac{\mathbb{D}(Q_1\|Q_0)}{\sqrt{\chi_2\left(Q_1\|Q_0\right)}}. \tag{4.132}$$

Note that the covert throughput in (4.131) *matches that of the point-to-point channel [27]. As a special case, we consider a broadcast setup for BSCs with* p_B *and* p_W *as the crossover probabilities for the channels from Alice to Bob and Willie, respectively. Assuming* $p_B \leqslant \frac{1}{2}$ *and* $p_W \leqslant \frac{1}{2}$ *without loss of generality, we obtain*

$$\mathbb{D}(P_1\|P_0) = \mathbb{D}(P_0\|P_1) = (1-2p_B)\log\left(\frac{1-p_B}{p_B}\right), \tag{4.133}$$

$$\mathbb{D}(Q_1\|Q_0) = \mathbb{D}(Q_0\|Q_1) = (1-2p_W)\log\left(\frac{1-p_W}{p_W}\right), \tag{4.134}$$

$$\chi_2\left(Q_1\|Q_0\right) = \chi_2\left(Q_0\|Q_1\right) = \frac{(1-2p_W)^2}{p_W\left(1-p_W\right)}. \tag{4.135}$$

Then, keyless covert communication is achievable in this channel model iff

$$(1-2p_B)\log\left(\frac{1-p_B}{p_B}\right) \geqslant (1-2p_W)\log\left(\frac{1-p_W}{p_W}\right). \tag{4.136}$$

Since $(1-2x)\log\left(\frac{1-x}{x}\right)$ *is a strictly decreasing function for* $x \in [0, \frac{1}{2}]$*, the condition in* (4.136) *translates to* $p_B \leqslant p_W$*. Hence, to embed covert information over a binary symmetric broadcast channel without using a secret key, the crossover probability of the channel to Bob cannot be greater than the crossover probability of the channel to Willie.*

4.6 Conclusion

We conclude this chapter by briefly discussing an extension of our results to non-binary input alphabets. Consider an input alphabet $\mathcal{X} \triangleq \{u\}_{u=0}^{K-1}$, where $K > 2$.

Note that, in our scenario, there is no notion of a *fixed innocent symbol*. We confirm that our results extend to non-binary input alphabets, and the steps required to arrive at our results are similar to those for the binary case discussed in this work. We denote the unique capacity-achieving input distribution for the channel to Willie by Λ, where $\Lambda(u) \triangleq \lambda_u *$ such that $\sum_{u=0}^{K-1} \lambda_u^* = 1$. We define two vectors $\boldsymbol{\gamma} \triangleq \{\gamma_u\}_{u\in[\![0,K-1]\!]} \in \mathbb{R}_+^K$ and $\boldsymbol{\beta} \triangleq \{\beta_{uv}\}_{(u,v)\in[\![0,K-1]\!]^2} \in [0,1]^{K^2}$ such that $\beta_{uu} = 0$, and $\sum_{v=0}^{K-1} \beta_{uv} = 1$ for all $u \in [\![0, K-1]\!]$. Then, following our proof techniques, one can show that we can achieve, for an arbitrary $\mu \in (0,1)$,

$$r_1 = (1-\mu) \max_{\boldsymbol{\gamma},\boldsymbol{\beta}} \sqrt{2} \frac{\sum_{u=0}^{K-1} \lambda_u^* \gamma_u \sum_{v=0}^{K-1} \beta_{uv} \mathbb{D}(P_v \| P_u)}{\sqrt{\sum_{u=0}^{K-1} \lambda_u^* \gamma_u^2 \chi_2\left(\sum_{v=0}^{K-1} \beta_{uv} Q_v \| Q_u\right)}}, \tag{4.137}$$

where the max in (4.137) is over all $\boldsymbol{\gamma}$ and $\boldsymbol{\beta}$ that satisfy

$$\sum_{u=0}^{K-1} \lambda_u^* \gamma_u \sum_{v=0}^{K-1} \beta_{uv} \mathbb{D}(P_v \| P_u) > \sum_{u=0}^{K-1} \lambda_u^* \gamma_u \sum_{v=0}^{K-1} \beta_{uv} \mathbb{D}(Q_v \| Q_u). \tag{4.138}$$

APPENDIX

4.A Proof of Lemma 8

Since $\overline{Q}_{\overline{\mathbf{x}},\alpha_n,\beta_n}^{\otimes n}$ is an n-fold distribution, we write $\overline{Q}_{\overline{\mathbf{x}},\alpha_n,\beta_n}^{\otimes n} = \prod_{i=1}^{n} \overline{Q}_{\overline{x}_i,\alpha_n,\beta_n}$. We now analyze the KL divergence between $\overline{Q}_{\overline{\mathbf{x}},\alpha_n,\beta_n}^{\otimes n}$ and $\overline{Q}_{\overline{\mathbf{x}},0,0}^{\otimes n}$.

$$\mathbb{D}\big(\overline{Q}_{\overline{\mathbf{x}},\alpha_n,\beta_n}^{\otimes n} \| \overline{Q}_{\overline{\mathbf{x}},0,0}^{\otimes n}\big) = \sum_{i=1}^{n} \mathbb{D}\big(\overline{Q}_{\overline{x}_i,\alpha_n,\beta_n} \| W_{Z|X=\overline{x}_i}\big) \tag{4.139}$$

$$= n\,(1-\lambda_n)\,\mathbb{D}\big(\overline{Q}_{0,\alpha_n,\beta_n} \| Q_0\big) + n\lambda_n \mathbb{D}\big(\overline{Q}_{1,\alpha_n,\beta_n} \| Q_1\big). \tag{4.140}$$

For $k \in \mathbb{N}^*$ and two distributions P and Q defined on the same alphabet $\mathcal{Z}$, we define $\chi_k\left(P\|Q\right) \triangleq \sum_z \frac{(P(z)-Q(z))^k}{Q^{k-1}(z)}$ and $\eta_k\left(P\|Q\right) \triangleq \sum_{z:P(z)-Q(z)<0} \frac{(P(z)-Q(z))^k}{Q^{k-1}(z)}$. Then, using [27, Lemma 1], we upper bound each of the two KL divergence terms in (4.140) by

$$\mathbb{D}\big(\overline{Q}_{0,\alpha_n,\beta_n} \| Q_0\big) \leqslant \frac{\alpha_n^2}{2}\chi_2\left(Q_1\|Q_0\right) - \frac{\alpha_n^3}{6}\chi_3\left(Q_1\|Q_0\right) + \frac{\alpha_n^4}{3}\chi_4\left(Q_1\|Q_0\right), \tag{4.141}$$

$$\mathbb{D}\big(\overline{Q}_{1,\alpha_n,\beta_n} \| Q_1\big) \leqslant \frac{\beta_n^2}{2}\chi_2\left(Q_0\|Q_1\right) - \frac{\beta_n^3}{6}\chi_3\left(Q_0\|Q_1\right) + \frac{\beta_n^4}{3}\chi_4\left(Q_0\|Q_1\right). \tag{4.142}$$

For n large enough, using [27, Lemma 1], we lower bound the two KL divergence terms in (4.140) by

$$\mathbb{D}\big(\overline{Q}_{0,\alpha_n,\beta_n} \| Q_0\big) \geqslant \frac{\alpha_n^2}{2}\chi_2\left(Q_1\|Q_0\right) - \alpha_n^3\left(\frac{1}{2}\chi_3\left(Q_1\|Q_0\right) - \frac{2}{3}\eta_3\left(Q_1\|Q_0\right)\right) + \frac{2\alpha_n^4}{3}\eta_4\left(Q_1\|Q_0\right), \tag{4.143}$$

$$\mathbb{D}\big(\overline{Q}_{1,\alpha_n,\beta_n} \| Q_1\big) \geqslant \frac{\beta_n^2}{2}\chi_2\left(Q_0\|Q_1\right) - \beta_n^3\left(\frac{1}{2}\chi_3\left(Q_0\|Q_1\right) - \frac{2}{3}\eta_3\left(Q_0\|Q_1\right)\right) + \frac{2\beta_n^4}{3}\eta_4\left(Q_0\|Q_1\right). \tag{4.144}$$

Loosening the bounds in (4.141)-(4.144), for n large enough, we obtain

$$\frac{\alpha_n^2}{2}\left(1+\sqrt{\alpha_n}\right)\chi_2\left(Q_1\|Q_0\right) \geqslant \mathbb{D}\big(\overline{Q}_{0,\alpha_n,\beta_n}\|Q_0\big) \geqslant \frac{\alpha_n^2}{2}\left(1-\sqrt{\alpha_n}\right)\chi_2\left(Q_1\|Q_0\right), \quad (4.145)$$

$$\frac{\beta_n^2}{2}\left(1+\sqrt{\beta_n}\right)\chi_2\left(Q_0\|Q_1\right) \geqslant \mathbb{D}\big(\overline{Q}_{1,\alpha_n,\beta_n}\|Q_1\big) \geqslant \frac{\beta_n^2}{2}\left(1-\sqrt{\beta_n}\right)\chi_2\left(Q_0\|Q_1\right). \quad (4.146)$$

Ultimately, combining (4.140), (4.145), and (4.146), we obtain (4.15).

4.B Proof of Lemma 10

We denote the covert transmission status of Alice by $T \triangleq 1 - \mathbb{1}\{W_1 = 0\}$ and Bob's estimate of T by $\widehat{T}$. For $j \in [\![1, M_2]\!]$ and $\mathbf{x}_{0j} \in \mathcal{C}_2$, define

$$\mathcal{A}_{\gamma_j}^n \triangleq \left\{(\mathbf{x},\mathbf{y}) \in \mathcal{X}^n \times \mathcal{Y}^n : \log \frac{W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x})}{\overline{P}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{y})} \geqslant \gamma_j\right\}, \quad (4.147)$$

where $\gamma_j > 0$ will be determined later. The decoder at Bob operates as follows

- if $\exists$ unique i such that $(\mathbf{x}_{ij},\mathbf{y}) \in \mathcal{A}_{\gamma_j}^n$, output $\widehat{W}_1 = i$,
- else if $\nexists\, i$ such that $(\mathbf{x}_{ij},\mathbf{y}) \in \mathcal{A}_{\gamma_j}^n$, output $\widehat{W}_1 = 0$,
- else, declare a decoding error.

Define the event $E_{ij} \triangleq \left\{(\mathbf{X}_{ij},\mathbf{Y}) \in \mathcal{A}_{\gamma_j}^n\right\}$. We also define

$$E_1 \triangleq \mathbb{E}_{\mathcal{C}}\left(\frac{1}{M_2}\sum_{j=1}^{M_2}\sum_{t'\in\{0,1\}}\mathbb{P}\Big(\widehat{T} \neq t' \Big| t = t', \widehat{W}_2 = W_2 = j\Big)\right), \quad (4.148)$$

$$E_2 \triangleq \mathbb{E}_{\mathcal{C}}\left(\frac{1}{M_2}\sum_{j=1}^{M_2}\mathbb{P}\Big(\widehat{W}_1 \neq W_1 \Big| \widehat{T} = t = 1, \widehat{W}_2 = W_2 = j\Big)\right). \quad (4.149)$$

The decoding error probability of the covert message averaged over all choices of the codebook $\mathcal{C}$ can be written as

$$\mathbb{E}_{\mathcal{C}}\left(\frac{1}{M_2}\sum_{j=1}^{M_2} P_{e,1,j}^{(1)}\right) = E_1 + E_2. \tag{4.150}$$

From the definition of E_1, we obtain

$$\begin{aligned} E_1 = \mathbb{E}_{\mathcal{C}}\left(\frac{1}{M_2}\sum_{j=1}^{M_2}\mathbb{P}\Big(\widehat{T}=0\Big|t=1,\widehat{W}_2=W_2=j\Big)\right) \\ + \mathbb{E}_{\mathcal{C}}\left(\frac{1}{M_2}\sum_{j=1}^{M_2}\mathbb{P}\Big(\widehat{T}=1\Big|t=0,\widehat{W}_2=W_2=j\Big)\right). \end{aligned} \tag{4.151}$$

We upper bound the first term in (4.151) by

$$\begin{aligned} &\mathbb{E}_{\mathcal{C}}\left(\frac{1}{M_2}\sum_{j=1}^{M_2}\mathbb{P}\Big(\widehat{T}=0\Big|t=1,\widehat{W}_2=W_2=j\Big)\right) \\ &= \mathbb{E}_{\mathcal{C}}\left(\frac{1}{M_1M_2}\sum_{j=1}^{M_2}\sum_{i=1}^{M_1}\sum_{\mathbf{y}} W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{X}_{ij})\mathbb{1}\left\{\bigcap_{i'} E_{i'j}^c\right\}\right) && (4.152) \\ &\overset{(a)}{\leqslant} \mathbb{E}_{\mathcal{C}}\left(\frac{1}{M_1M_2}\sum_{j=1}^{M_2}\sum_{i=1}^{M_1}\sum_{\mathbf{y}} W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{X}_{ij})\,\mathbb{1}\left\{E_{ij}^c\right\}\right) && (4.153) \\ &= \frac{1}{M_2}\sum_{j=1}^{M_2}\sum_{\mathbf{x}_{0j}} P_X^n(\mathbf{x}_{0j})\,\mathbb{P}_{W_{Y|X}^{\otimes n}\Pi_{\mathbf{x}_{0j},\alpha_n,\beta_n}}\left(\left(\mathcal{A}_{\gamma_j}^n\right)^c\right), && (4.154) \end{aligned}$$

where (a) follows from the fact that the probability of intersection of several events cannot exceed the probability of any one of those events. We bound the second term in (4.151) by

$$\begin{aligned} &\mathbb{E}_{\mathcal{C}}\left(\frac{1}{M_2}\sum_{j=1}^{M_2}\mathbb{P}\Big(\widehat{T}=1\Big|t=0,\widehat{W}_2=W_2=j\Big)\right) \\ &= \mathbb{E}_{\mathcal{C}}\left(\frac{1}{M_2}\sum_{j=1}^{M_2}\sum_{\mathbf{y}} W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{X}_{0j})\,\mathbb{1}\left\{\bigcup_{i} E_{ij}\right\}\right) && (4.155) \end{aligned}$$

$$\overset{(a)}{\leqslant} \frac{1}{M_2}\sum_{j=1}^{M_2}\sum_{\mathbf{x}_{0j}} P_X^n(\mathbf{x}_{0j}) \sum_{i=1}^{M_1}\sum_{\mathbf{y}}\sum_{\mathbf{x}_{ij}} W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x}_{0j})\Pi_{\mathbf{x}_{0j},\alpha_n,\beta_n}(\mathbf{x}_{ij})\mathbb{1}\left\{(\mathbf{x}_{ij},\mathbf{y})\in\mathcal{A}_{\gamma_j}^n\right\} \quad (4.156)$$

$$\leqslant \frac{1}{M_2}\sum_{j=1}^{M_2}\sum_{\mathbf{x}_{0j}} P_X^n(\mathbf{x}_{0j})\, M_1 e^{-\gamma_j}\sum_{\mathbf{y}}\sum_{\mathbf{x}_{1j}} \frac{W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x}_{1j})}{\overline{P}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{y})} W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x}_{0j})\,\Pi_{\mathbf{x}_{0j},\alpha_n,\beta_n}(\mathbf{x}_{1j}) \quad (4.157)$$

$$\overset{(b)}{\leqslant} \frac{1}{M_2}\sum_{j=1}^{M_2} M_1 e^{-\gamma_j}, \quad (4.158)$$

where (a) follows from the application of the union bound and (b) follows from the fact that $\sum_{\mathbf{x}_{1j}} W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{x}_{1j})\,\Pi_{\mathbf{x}_{0j},\alpha_n,\beta_n}(\mathbf{x}_{1j}) = \overline{P}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{y})$ and the definition of $\mathcal{A}_{\gamma_j}^n$. We then bound the second term in (4.150) by

$$E_2 \overset{(a)}{\leqslant} \mathbb{E}_{\mathcal{C}}\left(\frac{1}{M_1M_2}\sum_{j=1}^{M_2}\sum_{i=1}^{M_1}\sum_{\mathbf{y}} W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{X}_{ij})\,\mathbb{1}\{E_{ij}^c\}\right) + \mathbb{E}_{\mathcal{C}}\left(\frac{1}{M_1M_2}\sum_{j=1}^{M_2}\sum_{i=1}^{M_1}\sum_{\substack{i'=1\\ i'\neq i}}^{M_1}\sum_{\mathbf{y}} W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{X}_{ij})\mathbb{1}\{E_{i'j}\}\right), \quad (4.159)$$

where (a) follows from the union bound. We upper bound the second term in (4.159) by

$$\mathbb{E}_{\mathcal{C}}\left(\frac{1}{M_1M_2}\sum_{j=1}^{M_2}\sum_{i=1}^{M_1}\sum_{\substack{i'=1\\ i'\neq i}}^{M_1}\sum_{\mathbf{y}} W_{Y|X}^{\otimes n}(\mathbf{y}|\mathbf{X}_{ij})\mathbb{1}\{E_{i'j}\}\right)$$

$$\leqslant \frac{M_1}{M_2}\sum_{j=1}^{M_2}\sum_{\mathbf{x}_{0j}} P_X^n(\mathbf{x}_{0j})\sum_{\mathbf{y}}\sum_{\mathbf{x}_{1j}} \overline{P}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{y})\Pi_{\mathbf{x}_{0j},\alpha_n,\beta_n}(\mathbf{x}_{1j})\,\mathbb{1}\left\{(\mathbf{x}_{1j},\mathbf{y})\in\mathcal{A}_{\gamma_j}^n\right\} \quad (4.160)$$

$$\leqslant \frac{1}{M_2}\sum_{j=1}^{M_2} M_1 e^{-\gamma_j}. \quad (4.161)$$

Define $\gamma_j \triangleq (1-\delta)\sum_{i=1}^{n}\mathbb{I}\big(X_i;Y_i|\overline{X}_i=x_{0j,i}\big)$ for an arbitrary $\delta\in(0,1)$. Expanding $\mathbb{I}\big(X_i;Y_i|\overline{X}_i=x_{0j,i}\big)$, we obtain

$$\begin{aligned}
&\mathbb{I}\big(X_i;Y_i|\overline{X}_i=x_{0j,i}\big)\\
&=\left(\sum_y(1-\alpha_n)\,P_0(y)\log\frac{P_0(y)}{\overline{P}_{0,\alpha_n,\beta_n}(y)}+\sum_y\alpha_nP_1(y)\log\frac{P_1(y)}{\overline{P}_{0,\alpha_n,\beta_n}(y)}\right)\mathbb{1}\{x_{0j,i}=0\}\\
&\quad+\left(\sum_y\beta_nP_0(y)\log\frac{P_0(y)}{\overline{P}_{1,\alpha_n,\beta_n}(y)}+\sum_y(1-\beta_n)\,P_1(y)\log\frac{P_1(y)}{\overline{P}_{1,\alpha_n,\beta_n}(y)}\right)\mathbb{1}\{x_{0j,i}=1\} \qquad (4.162)\\
&=\big(\alpha_n\mathbb{D}(P_1\|P_0)-\mathbb{D}\big(\overline{P}_{0,\alpha_n,\beta_n}\|P_0\big)\big)\,\mathbb{1}\{x_{0j,i}=0\}\\
&\quad+\big(\beta_n\mathbb{D}(P_0\|P_1)-\mathbb{D}\big(\overline{P}_{1,\alpha_n,\beta_n}\|P_1\big)\big)\,\mathbb{1}\{x_{0j,i}=1\} \qquad (4.163)\\
&\overset{(a)}{=}\big(\alpha_n\mathbb{D}(P_1\|P_0)+\mathcal{O}\left(\alpha_n^2\right)\big)\,\mathbb{1}\{x_{0j,i}=0\}+\big(\beta_n\mathbb{D}(P_0\|P_1)+\mathcal{O}\left(\beta_n^2\right)\big)\,\mathbb{1}\{x_{0j,i}=1\}\,, \qquad (4.164)
\end{aligned}$$

where (a) follows from combining (4.141), (4.142), (4.143), and (4.144), in the proof of Lemma 8. Defining $\lambda_j \triangleq \sum_{i=1}^{n}\frac{\mathbb{1}\{x_{0j,i}=1\}}{n}$ and aggregating the n mutual information terms corresponding to each symbol position, we obtain

$$\begin{aligned}
\sum_{i=1}^{n}\mathbb{I}\big(X_i;Y_i|\overline{X}_i=x_{0j,i}\big)&=n\left((1-\lambda_j)\,\alpha_n\mathbb{D}(P_1\|P_0)+\lambda_j\beta_n\mathbb{D}(P_0\|P_1)\right)\\
&\quad+n\mathcal{O}\left(\alpha_n^2\right)+n\mathcal{O}\left(\beta_n^2\right). \qquad (4.165)
\end{aligned}$$

We bound the probability term in (4.154) by

$$\mathbb{P}_{W_{Y|X}^{\otimes n}\Pi_{\mathbf{x}_{0j},\alpha_n,\beta_n}}\left(\left(\mathcal{A}_{\gamma_j}^n\right)^c\right)\overset{(a)}{\leqslant}\exp\left(-\zeta_1n\alpha_n\right)+\exp\left(-\zeta_1n\beta_n\right), \qquad (4.166)$$

for an appropriate $\zeta_1>0$, where (a) follows from using Bernstein's inequality as in [69, Appendix D]. Then, combining (4.150), (4.151), (4.153), (4.154), (4.158), (4.159), (4.161), and (4.166), we infer that (4.36) is satisfied for a large n and an appropriate constant

$\xi_2 > 0$ if $\log M_1$ satisfies

$$\log M_1 < (1-\delta)\, n \left((1-\lambda_j)\, \alpha_n \mathbb{D}(P_1 \| P_0) + \lambda_j \beta_n \mathbb{D}(P_0 \| P_1) \right) + n\mathcal{O}\left(\alpha_n^2\right) + n\mathcal{O}\left(\beta_n^2\right), \tag{4.167}$$

for every $j \in [\![1, M_2]\!]$. Note that $\mathbf{x}_{0j}$ is generated according to P_X^n defined in (4.20). Hence, λ_j is arbitrarily close to λ^*. Combining this with the fact that δ is arbitrary, (4.36) is true if $\log M_1$ satisfies (4.35).

4.C Proof of Lemma 11

For $W_2 = j$ and $\mathbf{x}_{0j} \in \mathcal{C}_2$, define the set

$$\mathcal{B}_{\tau_j}^n \triangleq \left\{ (\mathbf{x}, \mathbf{z}) \in \mathcal{X}^n \times \mathcal{Z}^n : \log \frac{W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{x})}{\overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})} \leqslant \tau_j \right\}, \tag{4.168}$$

where $\tau_j > 0$ will be determined later. For a fixed $j \in [\![1, M_2]\!]$ and $i \in [\![1, M_1]\!]$, the expectation over all random codewords $\{\mathbf{X}_{kj}\}_{k \in [\![1,M_1]\!] \setminus \{i\}}$ is denoted by $\mathbb{E}_{\sim i}$. We bound the KL divergence between $\widehat{Q}_{W_2}^n$ and $\overline{Q}_{\mathbf{X}_{0W_2},\alpha_n,\beta_n}^{\otimes n}$ averaged over all choices of the common message W_2 and the codebook by

$$\begin{aligned}
&\mathbb{E}_{\mathcal{C}} \left(\mathbb{E}_{W_2} \mathbb{D}\Big(\widehat{Q}_{W_2}^n \| \overline{Q}_{\mathbf{X}_{0W_2},\alpha_n,\beta_n}^{\otimes n} \Big) \right) \\
&\quad = \mathbb{E}_{\mathcal{C}} \left(\frac{1}{M_2} \sum_{j=1}^{M_2} \sum_{\mathbf{z}} \frac{1}{M_1} \sum_{i=1}^{M_1} W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{X}_{ij}) \log \frac{\sum_{k=1}^{M_1} W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{X}_{kj})}{M_1 \overline{Q}_{\mathbf{X}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})} \right) \qquad (4.169) \\
&\quad = \frac{1}{M_1 M_2} \sum_{j=1}^{M_2} \sum_{i=1}^{M_1} \sum_{\mathbf{x}_{0j}} P_X^n(\mathbf{x}_{0j}) \sum_{\mathbf{z}} \sum_{\mathbf{x}_{ij}} W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{x}_{ij})\, \Pi_{\mathbf{x}_{0j},\alpha_n,\beta_n}(\mathbf{x}_{ij}) \\
&\qquad \times \mathbb{E}_{\sim i} \left(\log \left(\frac{\sum_{\substack{k=1 \\ k \neq i}}^{M_1} W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{X}_{kj})}{M_1 \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})} + \frac{W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{x}_{ij})}{M_1 \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})} \right) \right) \qquad (4.170)
\end{aligned}$$

$$\overset{(a)}{\leqslant} \frac{1}{M_1 M_2} \sum_{j=1}^{M_2} \sum_{i=1}^{M_1} \sum_{\mathbf{x}_{0j}} P_X^n(\mathbf{x}_{0j}) \sum_{\mathbf{z}} \sum_{\mathbf{x}_{ij}} W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{x}_{ij}) \, \Pi_{\mathbf{x}_{0j},\alpha_n,\beta_n}(\mathbf{x}_{ij}) \\ \times \log \mathbb{E}_{\sim i} \left(\frac{\sum_{\substack{k=1 \\ k\neq i}}^{M_1} W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{X}_{kj})}{M_1 \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})} + \frac{W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{x}_{ij})}{M_1 \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})} \right), \tag{4.171}$$

where (a) follows from Jensen's inequality. Define

$$\mu_{\min}^{(n)} \triangleq \min \left\{ (1-\alpha_n) \min_z Q_0(z), (1-\beta_n) \min_z Q_1(z) \right\}. \tag{4.172}$$

Now, we bound the log term in (4.171) by

$$\log \mathbb{E}_{\sim i} \left(\frac{\sum_{\substack{k=1 \\ k\neq i}}^{M_1} W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{X}_{kj})}{M_1 \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})} + \frac{W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{x}_{ij})}{M_1 \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})} \right)$$

$$= \log \left(\frac{\sum_{\substack{k=1 \\ k\neq i}}^{M_1} \sum_{\mathbf{x}_{kj}} W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{x}_{kj}) \, \Pi_{\mathbf{x}_{0j},\alpha_n,\beta_n}(\mathbf{x}_{kj})}{M_1 \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})} + \frac{W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{x}_{ij})}{M_1 \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})} \right) \tag{4.173}$$

$$\overset{(a)}{\leqslant} \log \left(1 + \frac{W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{x}_{ij})}{M_1 \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})} \right) \tag{4.174}$$

$$\leqslant \log \left(1 + \frac{e^{\tau_j}}{M_1} \right) + \log \left(1 + \frac{1}{\overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})} \right) \mathbb{1}\left\{ (\mathbf{x}_{ij}, \mathbf{z}) \notin \mathcal{B}_{\tau_j}^n \right\} \tag{4.175}$$

$$\leqslant \frac{e^{\tau_j}}{M_1} + n \log \left(\frac{2}{\mu_{\min}^{(n)}} \right) \mathbb{1}\left\{ (\mathbf{x}_{ij}, \mathbf{z}) \notin \mathcal{B}_{\tau_j}^n \right\}, \tag{4.176}$$

where (a) follows from the fact that $\sum_{\mathbf{x}_{kj}} W_{Z|X}^{\otimes n}(\mathbf{z}|\mathbf{x}_{kj}) \, \Pi_{\mathbf{x}_{0j},\alpha_n,\beta_n}(\mathbf{x}_{kj}) = \overline{Q}_{\mathbf{x}_{0j},\alpha_n,\beta_n}^{\otimes n}(\mathbf{z})$. Combining (4.171) and (4.176), we obtain

$$\mathbb{E}_{\mathcal{C}} \left(\mathbb{E}_{W_2} \mathbb{D}\left(\widehat{Q}_{W_2}^n \| \overline{Q}_{\mathbf{X}_{0W_2},\alpha_n,\beta_n}^{\otimes n} \right) \right) \\ \leqslant n \log \left(\frac{2}{\mu_{\min}^{(n)}} \right) \frac{1}{M_2} \sum_{j=1}^{M_2} \sum_{\mathbf{x}_{0j}} P_X^n(\mathbf{x}_{0j}) \, \mathbb{P}_{W_{Z|X}^{\otimes n} \Pi_{\mathbf{x}_{0j},\alpha_n,\beta_n}} \left(\left(\mathcal{B}_{\tau_j}^n \right)^c \right) + \frac{1}{M_2} \sum_{j=1}^{M_2} \frac{e^{\tau_j}}{M_1}. \tag{4.177}$$

Defining $\lambda_j \triangleq \sum_{i=1}^{n} \frac{\mathbb{1}\{x_{0j,i}=1\}}{n}$ and using steps similar to those used to obtain (4.165) in Appendix 4.B, we obtain

$$\sum_{i=1}^{n} \mathbb{I}\left(X_i; Z_i|\overline{X}_i = x_{0j,i}\right) = n\left((1-\lambda_j)\,\alpha_n \mathbb{D}(Q_1\|Q_0) + \lambda_j \beta_n \mathbb{D}(Q_0\|Q_1)\right) + n\mathcal{O}\left(\alpha_n^2\right) + n\mathcal{O}\left(\beta_n^2\right). \tag{4.178}$$

Defining $\tau_j \triangleq (1+\delta)\sum_{i=1}^{n} \mathbb{I}\big(X_i; Z_i|\overline{X}_i = x_{0j,i}\big)$ for an arbitrary $\delta > 0$, we bound the probability term on the right hand side of (4.177) using Bernstein's inequality 3.C by

$$\mathbb{P}_{W_{Z|X}^{\otimes n}\Pi_{\mathbf{x}_{0j},\alpha_n,\beta_n}}\left(\left(\mathcal{B}_{\tau_j}^n\right)^c\right) \leqslant \exp(-\zeta_2 n\alpha_n) + \exp(-\zeta_2 n\beta_n), \tag{4.179}$$

for an appropriate $\zeta_2 > 0$. Consequently, combining (4.177) and (4.179) and ensuring[5] $\log M_1$ satisfies (4.37) for an arbitrary $\nu \in (0,1)$ and a large n, we conclude that there exists a constant $\xi_3 > 0$ such that (4.38) is satisfied.

[5]Similar to Appendix 4.B, we remove the dependency of $\log M_1$ on j via λ_j in τ_j using the fact that λ_j is arbitrarily close to λ^* for every $j \in [\![1, M_2]\!]$ since $\mathbf{x}_{0j}$ is generated according to P_X^n defined in (4.20).

CHAPTER 5
COVERT COMMUNICATION OVER A PHYSICALLY DEGRADED RELAY CHANNEL WITH NON-COLLUDING WARDENS

5.1 Summary

In this chapter, we analyze a physically degraded relay channel, in which the transmitter sends a covert message to the legitimate receiver with the help of a relay. Two wardens, who do not collude with each other, monitor communication from the transmitter and the relay, respectively, through two Discrete Memoryless Channels (DMCs) to detect the transmission of a covert message. The objective of the transmitter is to deliver the covert message successfully to the receiver without exceeding the covertness threshold of either wardens. We identify the optimal asymptotic scaling of the message and key bits and the dependence of the number of covert bits on the two covert thresholds.

5.2 Introduction

Since any large communication network is fundamentally made up of multiple-access, broadcast, and relay channels, the analysis of covert communication over such models is of interest, especially when attempts to build entire covert networks on the horizon. In previous chapters, we characterized the information-theoretic limits of covert communication over multiple-access and broadcast channels [69, 80]. Following up, in this chapter, we show that the achievability and converse techniques developed in [27, 33, 69, 80] extend to physically degraded relay channels as well. We characterize the exact number of covert bits that can be transmitted over a physically degraded relay channel when communications from the transmitter and the relay are

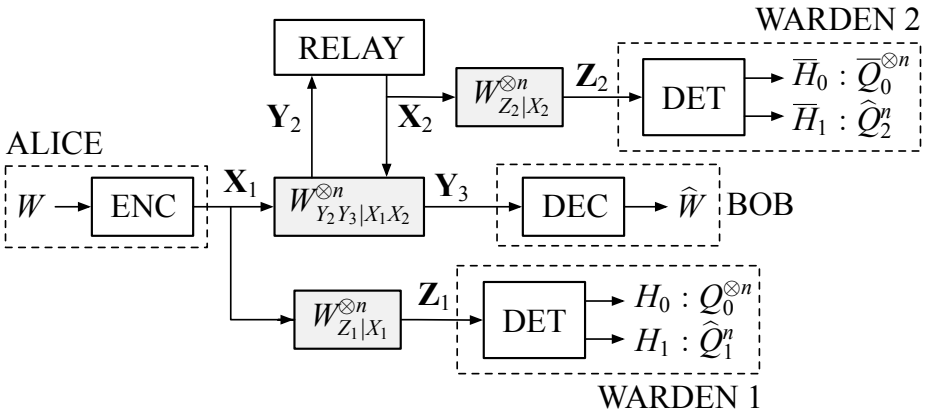

Figure 5.1: Model of covert communication over a physically degraded relay channel with two non-colluding wardens.

monitored by two non-colluding wardens. The presence of a second warden at the relay who monitors his communication is justified by the fact that a user who aids covert communication would want to keep his assistance covert as well.

A relay channel in which the relay communicates its own message covertly while hiding it from the transmitter, who also serves as the warden, is studied in [83]. In this case, the relay receives a sequence from the transmitter, adds his own covert message and relays the transmission to the receiver. Note that our channel model is significantly different, since in our case, the relay does not have its own covert message to send to the receiver. Moreover, [83] simplifies covertness analysis by using i.i.d. Gaussian codebooks.

The rest of the chapter is organized as follows. Section 5.3 introduces the channel model, and Section 5.4 presents our main result. The proofs are relegated to the appendix. This chapter is based on the results obtained in [84].

5.3 Channel Model

Consider the setup channel model illustrated in Figure 5.1. We consider a discrete memoryless relay channel $\left(\mathcal{X}_1, \mathcal{X}_2, W_{Y_2Y_3|X_1X_2}, \mathcal{Y}_2, \mathcal{Y}_3\right)$ that is physically degraded.

Then, for all x_1, x_2, y_2, y_3, $W_{Y_2Y_3|X_1X_2}$ decomposes as [85]

$$W_{Y_2Y_3|X_1X_2}(y_2, y_3|x_1, x_2) = W_{Y_2|X_1X_2}(y_2|x_1, x_2)W_{Y_3|Y_2X_2}(y_3|y_2, x_2). \tag{5.1}$$

As mentioned earlier, two wardens monitor the communication to detect covert transmissions. Warden 1 monitors transmissions from Alice, the transmitter, through a DMC $\left(\mathcal{X}_1, W_{Z_1|X_1}, \mathcal{Z}_1\right)$, and Warden 2 monitors transmissions from the relay through another DMC $\left(\mathcal{X}_2, W_{Z_2|X_2}, \mathcal{Z}_2\right)$. We assume binary input alphabets for both the transmitter and the relay, that is, $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{X} \triangleq \{0, 1\}$. We fix 0 as the innocent symbol, that is, the channel input when no communication occurs. We also assume finite output alphabets. For $a, b \in \{0, 1\}$, we denote the output distributions at the relay and at Bob, the receiver, respectively by

$$\overline{P}_{ab}(y_2) \triangleq W_{Y_2|X_1X_2}(y_2|a, b), \tag{5.2}$$

$$P_{ab}(y_3) \triangleq W_{Y_3|X_1X_2}(y_3|a, b), \tag{5.3}$$

for $y_2 \in \mathcal{Y}_2$ and $y_3 \in \mathcal{Y}_3$. On a related note, for $a \in \{0, 1\}$, we define the output distributions at the two wardens, respectively, by

$$Q_a(z_1) \triangleq W_{Z_1|X_1}(z_1|a), \tag{5.4}$$

$$\overline{Q}_a(z_2) \triangleq W_{Z_2|X_2}(z_2|a), \tag{5.5}$$

for $z_1 \in \mathcal{Z}_1$ and $z_2 \in \mathcal{Z}_2$. For reasons discussed in [27] and previous chapters, we assume that $P_{ab} \ll P_{00}$ and $\overline{P}_{ab} \ll \overline{P}_{00}$ for all $a, b \in \{0, 1\}$. We also assume that $Q_1 \ll Q_0$, $\overline{Q}_1 \ll \overline{Q}_0$, $Q_1 \neq Q_0$, and $\overline{Q}_1 \neq \overline{Q}_0$ as in [27].

Alice wants to communicate a covert message W uniformly distributed in $[\![1, M]\!]$ to Bob with the help of a relay and a secret key that is uniformly distributed in $[\![1, K]\!]$. Alice maps the covert message and the key to a transmission sequence $\mathbf{X}_1$.

The relay generates the current symbol based on his past observations; that is, $X_{2,i}$ is a function of the observed sequence $(Y_{2,1}, \ldots, Y_{2,i-1})$ and the shared key S. Upon observing the entire output sequence $\mathbf{Y}_3$, Bob uses $\mathbf{Y}_3$ and the shared key to estimate the covert message as $\widehat{W}$. We measure reliability at Bob by the error probability $P_e \triangleq \mathbb{P}\Big(\widehat{W} \neq W\Big)$. Wardens 1 and 2 observe sequences $\mathbf{Z}_1$ and $\mathbf{Z}_2$, respectively. We denote the distributions induced at the two wardens when communication takes place by $\widehat{Q}_1^n$ and $\widehat{Q}_2^n$, respectively. Furthermore, we measure covertness at the wardens in terms of the respective KL divergences, $\mathbb{D}\Big(\widehat{Q}_1^n \| Q_0^{\otimes n}\Big)$ and $\mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_0^{\otimes n}\Big)$. If the communication scheme used by Alice ensures that both the KL divergence terms above are below the respective covert thresholds, then any statistical test used by the wardens is futile in detecting the presence of a covert message. The objective of Alice is to transmit such that, for $\delta_1, \delta_2 > 0$,

$$\lim_{n\to\infty} P_e = 0, \tag{5.6}$$

$$\limsup_{n\to\infty} \mathbb{D}\Big(\widehat{Q}_1^n \| Q_0^{\otimes n}\Big) \leqslant \delta_1, \tag{5.7}$$

$$\limsup_{n\to\infty} \mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_0^{\otimes n}\Big) \leqslant \delta_2. \tag{5.8}$$

We refer to δ_1 and δ_2 in (5.7) and (5.8) as the covertness thresholds of wardens 1 and 2, respectively. In a sense, covertness thresholds can be understood as tolerances of the wardens. Unlike previous chapters, in this chapter, we do not require that the covertness measure to vanish in the limit of large blocklength. In order to understand how the covert thresholds affect the number of reliable and covert bits that can be transmitted with the help of a relay, we characterize the exact scaling of $\log M$ and $\log K$ with n in terms of $\delta_1, \delta_2 > 0$, such that (5.6), (5.7), and (5.8) are all satisfied.

5.4 Main result

In this section, we present our main result in Theorem 5 and provide an achievability and a converse proof. First, we define chi-square distances at the two wardens by

$$\chi_2 \triangleq \sum_{z_1 \in \mathcal{Z}_1} \frac{\left(Q_1(z_1) - Q_0(z_1)\right)^2}{Q_0(z_1)} 2, \tag{5.9}$$

$$\overline{\chi}_2 \triangleq \sum_{z_2 \in \mathcal{Z}_2} \frac{\left(\overline{Q}_1(z_2) - \overline{Q}_0(z_2)\right)^2}{\overline{Q}_0(z_2)}. \tag{5.10}$$

For any $\gamma \geqslant 0$ and $\beta \in [0,1]$, we define

$$\Gamma(\gamma,\beta) \triangleq \min\left(\frac{1}{(1+\gamma\beta)}\sqrt{\frac{\delta_1}{\chi_2}}, \frac{1}{\gamma}\sqrt{\frac{\delta_2}{\overline{\chi}_2}}\right), \tag{5.11}$$

$$\begin{aligned}\zeta_1(\gamma,\beta) \triangleq\ & \mathbb{D}\big(\overline{P}_{10}\|\overline{P}_{00}\big) + \gamma(1-\beta)\mathbb{D}\big(\overline{P}_{01}\|\overline{P}_{00}\big) + \gamma\beta\mathbb{D}\big(\overline{P}_{11}\|\overline{P}_{00}\big) \\ & - \gamma\mathbb{D}\big((1-\beta)\overline{P}_{01} + \beta\overline{P}_{11}\|\overline{P}_{00}\big),\end{aligned} \tag{5.12}$$

$$\zeta_2(\gamma,\beta) \triangleq \mathbb{D}(P_{10}\|P_{00}) + \gamma(1-\beta)\mathbb{D}(P_{01}\|P_{00}) + \gamma\beta\mathbb{D}(P_{11}\|P_{00}). \tag{5.13}$$

We also define

$$\kappa_1(\gamma,\beta) \triangleq \min\left(\zeta_1(\gamma,\beta), \zeta_2(\gamma,\beta)\right), \tag{5.14}$$

$$\kappa_2(\gamma,\beta) \triangleq \max\Big((1+\gamma\beta)\,\mathbb{D}(Q_1\|Q_0), \gamma\mathbb{D}\big(\overline{Q}_1\|\overline{Q}_0\big)\Big), \tag{5.15}$$

to represent our results in a concise manner. Our main result is the following.

Theorem 5. *For the degraded channel model described in Section 5.3, let $M^*(n,\epsilon)$ be the largest possible value of M such that an n-length channel code can be constructed to satisfy* (5.7), (5.8), *and $P_e \leq \epsilon$. Then,*

$$\lim_{\epsilon\downarrow 0}\lim_{n\to\infty}\frac{\log M^*(n,\epsilon)}{\sqrt{n}} = \sup_{\substack{\gamma\geqslant 0,\\ \beta\in[0,1]}} \sqrt{2}\Gamma(\gamma,\beta)\,\kappa_1(\gamma,\beta). \tag{5.16}$$

Furthermore, this optimal scaling can be achieved if

$$\liminf_{n\to\infty} \frac{\log K}{\sqrt{n}} > \sqrt{2}\Gamma\left(\gamma^*, \beta^*\right)[\kappa_2\left(\gamma^*, \beta^*\right) - \kappa_1\left(\gamma^*, \beta^*\right)]^+, \tag{5.17}$$

and only if

$$\liminf_{n\to\infty} \frac{\log K}{\sqrt{n}} \geqslant \sqrt{2}\Gamma\left(\gamma^*, \beta^*\right)[\kappa_2\left(\gamma^*, \beta^*\right) - \kappa_1\left(\gamma^*, \beta^*\right)]^+, \tag{5.18}$$

for some (γ^*, β^*) *pair that achieves the limit in* (5.16)*.*

Note that both $\Gamma(\gamma, \beta)\kappa_1(\gamma, \beta)$ and $\Gamma(\gamma, \beta)\kappa_2(\gamma, \beta)$ are bounded for all $\gamma \geqslant 0$ and $\beta \in [0, 1]$. If there exist multiple (γ^*, β^*) pairs, we choose the pair that minimizes the lower bound in (5.18), that is, we choose the pair that needs the least amount of secret key to be shared.

Remark 3. *If* $\gamma^* = 0$*, we have*

$$\Gamma(0, \beta^*) = \sqrt{\frac{\delta_1}{\chi_2}}, \tag{5.19}$$

$$\kappa_1(0, \beta^*) = \mathbb{D}(P_{10} \| P_{00}). \tag{5.20}$$

since $\mathbb{D}\big(\overline{P}_{10} \| \overline{P}_{00}\big) \geqslant \mathbb{D}(P_{10} \| P_{00})$ *due to the degraded channel assumption. Consequently, we have*

$$\lim_{\epsilon \downarrow 0} \lim_{n\to\infty} \frac{\log M^*(n, \epsilon)}{\sqrt{n}} = \sqrt{\frac{2\delta_1}{\chi_2}} \mathbb{D}(P_{10} \| P_{00}), \tag{5.21}$$

which matches the covert throughput achieved when the relay is not used to forward any covert information [27], that is, when information only flows directly from Alice to Bob.

In the two subsections that follow, we describe a covert communication scheme

that achieves the optimal covert throughput in (5.16) and a converse that proves that the achievable scheme discussed is asymptotically optimal.

5.4.1 Proof of achievability for Theorem 5

In our communication scheme, we use a block-Markovian encoding scheme at Alice and the relay encoder, and a sliding-window decoding scheme at Bob. We follow the decode-and-forward scheme detailed in [86] with slight modifications to ensure covertness at the wardens. For $B \in \mathbb{N}^*$, divide the message $m \in [\![1, M]\!]$ into B equal-sized messages $\mathbf{m}_1^B$ each of length $\log M'$, where $\log M' = \frac{\log M}{B}$. Also, divide the key $k \in [\![1, K]\!]$ into $B+1$ parts: $\mathbf{k}_1^B$, each of length $\log K'$, and another part $\hat{k}$. We specify $\log K'$ and the length of $\hat{k}$ later. Alice randomly chooses a pair $(m_0, k_0) \in [\![1, M']\!] \times [\![1, K']\!]$ and reveals it to Bob and the relay. Note that, unlike block-Markovian encoding in traditional problems [85, 86], m_0 cannot be fixed in advance, because the warden can detect a fixed codeword with ease. To this end, we employ the key $\hat{k}$ to reveal the message-key pair (m_0, k_0) to the relay and Bob. Note that $\hat{k}$ is of length $\log M' + \log K'$. Consequently, we have

$$\log K = (B+1) \log K' + \log M'. \tag{5.22}$$

However, as B grows, $\log K$ approximately equals $B \log K'$. Next, for $n \in \mathbb{N}^*$, define

$$\alpha_n \triangleq \sqrt{\frac{2}{n}} \cdot \Gamma(\gamma, \beta), \tag{5.23}$$

and fix $\gamma \geqslant 0$ and $\beta \in [0, 1]$ such that $\alpha_n \in (0, 1)$. For a large n, define the input distribution Π_{X_2} by

$$\Pi_{X_2}(1) = 1 - \Pi_{X_2}(0) = \gamma \alpha_n, \tag{5.24}$$

and the conditional distribution $\Pi_{X_1|X_2}$ by

$$\Pi_{X_1|X_2}(1|0) = 1 - \Pi_{X_1|X_2}(0|0) = \alpha_n, \tag{5.25}$$

$$\Pi_{X_1|X_2}(1|1) = 1 - \Pi_{X_1|X_2}(0|1) = \beta. \tag{5.26}$$

Note that while α_n is a function of n, $\beta \in [0,1]$ is a constant. Furthermore, defining $\rho_n \triangleq 1 + \gamma\beta - \gamma\alpha_n$ and combining (5.24), (5.25), and (5.26), we have

$$\Pi_{X_1}(1) = \rho_n \alpha_n. \tag{5.27}$$

Since $\lim_{n\to\infty} \alpha_n = 0$, we have $\lim_{n\to\infty} \rho_n = 1 + \gamma\beta$.

Next, we generate a separate codebook $\mathcal{C}_b$ for each block $b \in [\![1, B+1]\!]$. We define $N \triangleq \frac{n}{B+1}$. For block b, first generate $M'K'$ codewords $\mathbf{x}_{2b,k}(m)$ each of length N, where $m \in [\![1, M']\!]$ and $k \in [\![1, K']\!]$, according to the distribution $\Pi_{X_2}^{\otimes N}$. Then, for each $\mathbf{x}_{2b,s}(w)$, generate $M'K'$ codewords $\mathbf{x}_{1b,(k,k')}(m, m')$ of length N, where $m, m' \in [\![1, M']\!]$ and $k, k' \in [\![1, K']\!]$, conditionally independently according to the distribution $\Pi_{X_1|X_2}^{\otimes N}(\cdot|\mathbf{x}_{2b,k}(m))$. In transmission block b, Bob and the relay observe the N-length sequences $\mathbf{y}_{2b}$ and $\mathbf{y}_{3b}$, respectively. Similarly, the wardens observe the N-length sequences $\mathbf{z}_{1b}$ and $\mathbf{z}_{2b}$, respectively, in block b. We fix $m_{B+1} = k_{B+1} = 1$ and reveal this choice to all users. We also reveal the collection of codebooks $\mathcal{C} \triangleq \{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_{B+1}\}$ to all users.

Defining

$$\mathcal{A}_{\eta_1}^N \triangleq \left\{ (\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}_2) \in \mathcal{X}^N \times \mathcal{X}^N \times \mathcal{Y}_2^N : \log \frac{W_{Y_2|X_1X_2}^{\otimes N}(\mathbf{y}_2|\mathbf{x}_1\mathbf{x}_2)}{P_{Y_2|X_2}^{\otimes N}(\mathbf{y}_2|\mathbf{x}_2)} \geqslant \eta_1 \right\}, \tag{5.28}$$

$$\mathcal{A}_{\eta_{21}}^N \triangleq \left\{ (\mathbf{x}_1, \mathbf{x}_2, \mathbf{y}_3) \in \mathcal{X}^N \times \mathcal{X}^N \times \mathcal{Y}_3^N : \log \frac{W_{Y_3|X_1X_2}^{\otimes N}(\mathbf{y}_3|\mathbf{x}_1\mathbf{x}_2)}{P_{Y_3|X_2}^{\otimes N}(\mathbf{y}_3|\mathbf{x}_2)} \geqslant \eta_{21} \right\}, \tag{5.29}$$

$$\mathcal{A}_{\eta_{22}}^N \triangleq \left\{ (\mathbf{x}_2, \mathbf{y}_3) \in \mathcal{X}^N \times \mathcal{Y}_3^N : \log \frac{P_{Y_3|X_2}^{\otimes N}(\mathbf{y}_3|\mathbf{x}_2)}{P_{Y_3}^{\otimes N}(\mathbf{y}_3)} \geqslant \eta_{22} \right\}, \tag{5.30}$$

we define the sets

$$\mathcal{A}_{\eta}^{N} \triangleq \mathcal{A}_{\eta_1}^{N} \cap \mathcal{A}_{\eta_{21}}^{N} \cap \mathcal{A}_{\eta_{22}}^{N}, \tag{5.31}$$

$$\mathcal{A}_{\eta_2}^{N} \triangleq \mathcal{A}_{\eta_{21}}^{N} \cap \mathcal{A}_{\eta_{22}}^{N}, \tag{5.32}$$

We specify the exact values of η_1, η_{21}, and η_{22} later.

Encoding and decoding

- In block b, Alice encodes the message pair $(m_{b-1}, m_b) \in [\![1, M']\!]^2$ and the key pair $(k_{b-1}, k_b) \in [\![1, K']\!]^2$ into the codeword $\mathbf{x}_{1b,(k_{b-1},k_b)}(m_{b-1}, m_b)$.

- In transmission block b, the relay observes $\mathbf{y}_{2b}$ and finds an estimate $\widetilde{m}_b$ such that $\left(\mathbf{x}_{1b,(k_{b-1},k_b)}\left(\widetilde{m}_{b-1}, \widetilde{m}_b\right), \mathbf{x}_{2b,k_{b-1}}\left(\widetilde{m}_{b-1}\right), \mathbf{y}_{2b}\right) \in \mathcal{A}_{\eta_1}^{N}$, where $\widetilde{m}_{b-1}$ is the relay's estimate of m_{b-1} in the previous block $b-1$.

- If multiple $\widetilde{m}_b$ are found, the relay chooses one among them at random; if none are found, the relay sets $\widetilde{m}_b = 1$.

- The relay encodes its estimate $\widetilde{m}_b$ into codeword $\mathbf{x}_{2(b+1),k_b}(\widetilde{m}_b)$ and transmits it in transmission block $b+1$.

- Bob uses a block-sliding window decoder of length $2n$ spanning two blocks at any point of time.

- Bob observes $\mathbf{y}_{3(b-1)}$ and $\mathbf{y}_{3b}$ during blocks $b-1$ and b, respectively, and finds an estimate $\widehat{m}_{b-1}$ such that $\left(\mathbf{x}_{1(b-1),(k_{b-2},k_{b-1})}\left(\widehat{m}_{b-2}, \widehat{m}_{b-1}\right), \mathbf{x}_{2(b-1),k_{b-2}}\left(\widehat{m}_{b-2}\right), \mathbf{y}_{3(b-1)}\right) \in \mathcal{A}_{\eta_{21}}^{N}$ and $\left(\mathbf{x}_{2b,k_{b-1}}(\widehat{m}_{b-1}), \mathbf{y}_{3b}\right) \in \mathcal{A}_{\eta_{22}}^{N}$, where $\widehat{m}_{b-2}$ is Bob's estimate in the previous block.

- If multiple $\widehat{m}_{b-1}$ are found, Bob chooses one among them at random; if none are found, Bob sets $\widehat{m}_{b-1} = 1$.

Reliability Analysis The decoding error probability P_e averaged over all random codebooks satisfies the following lemma.

Lemma 12. *For an arbitrary $\mu \in (0,1)$, a large N, and*

$$\log M = (1-\mu)\, n \frac{B}{B+1} \alpha_n \kappa_1 (\gamma, \beta), \tag{5.33}$$

the probability of decoding error averaged over all random codebooks $\mathcal{C}$ is

$$\mathbb{E}_{\mathcal{C}} (P_e) \leqslant \exp(-cN\alpha_n), \tag{5.34}$$

for an appropriate constant $c > 0$.

Note that the fraction $\frac{B}{B+1}$ approximates 1 as B becomes large. The proof of Lemma 12 is provided in Appendix 5.A.

Resolvability analysis Following our approach [27] of first defining a covert process that is indistinguishable from the innocent distribution and then designing a communication scheme that induces a distribution close to the covert process, we define the covert processes at the two wardens by

$$Q_{\alpha_n}(z_1) \triangleq \sum_{x_1} W_{Z_1|X_1}(z_1|x_1) \Pi_{X_1}(x_1), \tag{5.35}$$

$$\overline{Q}_{\alpha_n}(z_2) \triangleq \sum_{x_2} W_{Z_2|X_2}(z_2|x_2) \Pi_{X_2}(x_2), \tag{5.36}$$

respectively. We denote the corresponding n-fold product distributions by

$$\Pi_{X_1X_2}^{\otimes n} \triangleq \prod_{i=1}^{n} \Pi_{X_1X_2},\ Q_{\alpha_n}^{\otimes n} \triangleq \prod_{i=1}^{n} Q_{\alpha_n},\ \overline{Q}_{\alpha_n}^{\otimes n} \triangleq \prod_{i=1}^{n} \overline{Q}_{\alpha_n}. \tag{5.37}$$

Using steps similar to the ones in [27, Lemma 1] and previous chapters, we obtain

$$\frac{\rho_n^2\alpha_n^2}{2}\left(1+\sqrt{\rho_n\alpha_n}\right)\chi_2 \geqslant \mathbb{D}(Q_{\alpha_n}\|Q_0) \geqslant \frac{\rho_n^2\alpha_n^2}{2}\left(1-\sqrt{\rho_n\alpha_n}\right)\chi_2, \tag{5.38}$$

$$\frac{\gamma^2\alpha_n^2}{2}\left(1+\sqrt{\gamma\alpha_n}\right)\overline{\chi}_2 \geqslant \mathbb{D}\big(\overline{Q}_{\alpha_n}\|\overline{Q}_0\big) \geqslant \frac{\gamma^2\alpha_n^2}{2}\left(1-\sqrt{\gamma\alpha_n}\right)\overline{\chi}_2. \tag{5.39}$$

Our choice of α_n in (5.23) results in

$$\lim_{n\to\infty}\mathbb{D}\big(Q_{\alpha_n}^{\otimes n}\|Q_0^{\otimes n}\big) = \lim_{n\to\infty} n\mathbb{D}(Q_{\alpha_n}\|Q_0) \tag{5.40}$$

$$= 2\Gamma(\gamma,\beta)^2\cdot\frac{(1+\gamma\beta)^2}{2}\chi_2 \tag{5.41}$$

$$\leqslant \delta_1, \tag{5.42}$$

where (5.42) follows from the definition of $\Gamma(\gamma,\beta)$ in (5.11). Similarly, we have

$$\lim_{n\to\infty}\mathbb{D}\Big(\overline{Q}_{\alpha_n}^{\otimes n}\|\overline{Q}_0^{\otimes n}\Big) = \lim_{n\to\infty} n\mathbb{D}\big(\overline{Q}_{\alpha_n}\|\overline{Q}_0\big) \tag{5.43}$$

$$= 2\Gamma(\gamma,\beta)^2\cdot\frac{\gamma^2}{2}\overline{\chi}_2 \tag{5.44}$$

$$\leqslant \delta_2. \tag{5.45}$$

It then remains to show that the induced distributions at the two non-colluding wardens are indistinguishable from the respective covert processes. The gist of our approach is to use channel resolvability techniques to ensure that the codebook $\mathcal{C}_b$ for each transmission block has sufficiently enough codewords to confuse both wardens, while simultaneously ensuring reliable decoding at Bob. In the following lemma, we show that the KL divergence between the induced distribution and the respective covert process at each warden is small.

Lemma 13. *For an arbitrary $\mu\in(0,1)$, a large N, and*

$$\log M + \log K = (1+\mu)n\alpha_n\kappa_2(\gamma,\beta), \tag{5.46}$$

the KL divergence between the induced distribution and the respective covert processes at the two wardens averaged over all random codebooks is

$$\mathbb{E}_{\mathcal{C}}\left(\mathbb{D}\Big(\widehat{Q}_1^n \| Q_{\alpha_n}^{\otimes n}\Big)\right) \leqslant \exp\left(-cn\alpha_n\right), \tag{5.47}$$

$$\mathbb{E}_{\mathcal{C}}\left(\mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_{\alpha_n}^{\otimes n}\Big)\right) \leqslant \exp\left(-cn\alpha_n\right), \tag{5.48}$$

for an appropriate constant $c > 0$.

The proof of Lemma 13 is provided in Appendix 5.B.

Identification of a specific code Let us now consider the probability that for a particular coding scheme, the error probability and KL divergences at both wardens are simultaneously less than six times their respective expected values.

$$\begin{aligned}
&\mathbb{P}\left(P_e < 6\mathbb{E}\left(P_e\right) \cap \mathbb{D}\Big(\widehat{Q}_1^n \| Q_{\alpha_n}^{\otimes n}\Big) < 6\mathbb{E}\left(\mathbb{D}\Big(\widehat{Q}_1^n \| Q_{\alpha_n}^{\otimes n}\Big)\right)\right. \\
&\qquad \left.\bigcap \mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_{\alpha_n}^{\otimes n}\Big) < 6\mathbb{E}\left(\mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_{\alpha_n}^{\otimes n}\Big)\right)\right) \\
&= 1 - \mathbb{P}\left(P_e \geqslant 6\mathbb{E}\left(P_e\right) \cup \mathbb{D}\Big(\widehat{Q}_1^n \| Q_{\alpha_n}^{\otimes n}\Big) \geqslant 6\mathbb{E}\left(\mathbb{D}\Big(\widehat{Q}_1^n \| Q_{\alpha_n}^{\otimes n}\Big)\right)\right. \\
&\qquad \left.\bigcup \mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_{\alpha_n}^{\otimes n}\Big) \geqslant 6\mathbb{E}\left(\mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_{\alpha_n}^{\otimes n}\Big)\right)\right) \qquad (5.49) \\
&\geqslant 1 - \mathbb{P}(P_e \geqslant 6\mathbb{E}\left(P_e\right)) - \mathbb{P}\left(\mathbb{D}\Big(\widehat{Q}_1^n \| Q_{\alpha_n}^{\otimes n}\Big) \geqslant 6\mathbb{E}\left(\mathbb{D}\Big(\widehat{Q}_1^n \| Q_{\alpha_n}^{\otimes n}\Big)\right)\right) \\
&\qquad - \mathbb{P}\left(\mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_{\alpha_n}^{\otimes n}\Big) \geqslant 6\mathbb{E}\left(\mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_{\alpha_n}^{\otimes n}\Big)\right)\right) \qquad (5.50) \\
&\overset{(a)}{\geqslant} \frac{1}{2}, \qquad (5.51)
\end{aligned}$$

where (a) follows from Markov's inequality. From (5.51), we conclude that there must exist at least one coding scheme such that, for a large n and appropriate constants

$c_1, c_2, c_3 > 0$,

$$P_e \leqslant \exp(-c_1 n\alpha_n), \tag{5.52}$$

$$\mathbb{D}\Big(\widehat{Q}_1^n \| Q_{\alpha_n}^{\otimes n}\Big) \leqslant \exp(-c_2 n\alpha_n), \tag{5.53}$$

$$\mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_{\alpha_n}^{\otimes n}\Big) \leqslant \exp(-c_3 n\alpha_n). \tag{5.54}$$

We upper bound the KL divergence between $\widehat{Q}_1^n$ and $Q_0^{\otimes n}$ by

$$\mathbb{D}\Big(\widehat{Q}_1^n \| Q_0^{\otimes n}\Big) = \mathbb{D}\Big(\widehat{Q}_1^n \| Q_{\alpha_n}^{\otimes n}\Big) + \sum_{\mathbf{z}} \widehat{Q}_1^n(\mathbf{z}) \log \frac{Q_{\alpha_n}^{\otimes n}(\mathbf{z})}{Q_0^{\otimes n}(\mathbf{z})} \tag{5.55}$$

$$= \mathbb{D}\Big(\widehat{Q}_1^n \| Q_{\alpha_n}^{\otimes n}\Big) + \mathbb{D}\big(Q_{\alpha_n}^{\otimes n} \| Q_0^{\otimes n}\big) + \sum_{\mathbf{z}} \Big(\widehat{Q}_1^n(\mathbf{z}) - Q_{\alpha_n}^{\otimes n}(\mathbf{z})\Big) \log \frac{Q_{\alpha_n}^{\otimes n}(\mathbf{z})}{Q_0^{\otimes n}(\mathbf{z})} \tag{5.56}$$

$$\leqslant \mathbb{D}\Big(\widehat{Q}_1^n \| Q_{\alpha_n}^{\otimes n}\Big) + \mathbb{D}\big(Q_{\alpha_n}^{\otimes n} \| Q_0^{\otimes n}\big) + \left| \sum_{\mathbf{z}} \Big(\widehat{Q}_1^n(\mathbf{z}) - Q_{\alpha_n}^{\otimes n}(\mathbf{z})\Big) \log \frac{Q_{\alpha_n}^{\otimes n}(\mathbf{z})}{Q_0^{\otimes n}(\mathbf{z})} \right| \tag{5.57}$$

$$\leqslant \mathbb{D}\Big(\widehat{Q}_1^n \| Q_{\alpha_n}^{\otimes n}\Big) + \mathbb{D}\big(Q_{\alpha_n}^{\otimes n} \| Q_0^{\otimes n}\big) + \mathbb{V}\Big(\widehat{Q}_1^n, Q_{\alpha_n}^{\otimes n}\Big) n \log \frac{1}{\mu_1} \tag{5.58}$$

$$\overset{(a)}{\leqslant} \exp(-c_2 n\alpha_n) + \mathbb{D}\big(Q_{\alpha_n}^{\otimes n} \| Q_0^{\otimes n}\big) + n \log \frac{1}{\mu_1} \exp\Big(-\frac{c_2}{2} n\alpha_n\Big) \tag{5.59}$$

where (a) follows from (5.53) and the fact that $\mathbb{V}\Big(\widehat{Q}_1^n, Q_{\alpha_n}^{\otimes n}\Big) \leqslant \exp\big(-\frac{c_2 n\alpha_n}{2}\big)$. Applying limits to (5.59), we obtain

$$\limsup_{n\to\infty} \mathbb{D}\Big(\widehat{Q}_1^n \| Q_0^{\otimes n}\Big) \leqslant \lim_{n\to\infty} \mathbb{D}\big(Q_{\alpha_n}^{\otimes n} \| Q_0^{\otimes n}\big). \tag{5.60}$$

Using similar steps, we can obtain

$$\limsup_{n\to\infty} \mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_0^{\otimes n}\Big) \leqslant \lim_{n\to\infty} \mathbb{D}\Big(\overline{Q}_{\alpha_n}^{\otimes n} \| \overline{Q}_0^{\otimes n}\Big). \tag{5.61}$$

Since $\lim_{n\to\infty} \mathbb{D}\big(Q_{\alpha_n}^{\otimes n} \| Q_0^{\otimes n}\big) \leqslant \delta_1$ and $\lim_{n\to\infty} \mathbb{D}\Big(\overline{Q}_{\alpha_n}^{\otimes n} \| \overline{Q}_0^{\otimes n}\Big) \leqslant \delta_2$, our communication scheme satisfies the covertness constraints in (5.7) and (5.8).

Asymptotic behavior Let us now characterize the asymptotic scaling of $\log M$ for the covert communication scheme that we just discussed. We normalize (5.33) by $\sqrt{n}$ and apply limits to obtain

$$\lim_{n\to\infty} \frac{\log M}{\sqrt{n}} = (1-\mu) \lim_{n\to\infty} \left(\sqrt{n}\alpha_n\right) \frac{B}{B+1} \kappa_1(\gamma,\beta) \tag{5.62}$$

$$= (1-\mu)\sqrt{2} \frac{B}{B+1} \Gamma(\gamma,\beta)\, \kappa_1(\gamma,\beta) \tag{5.63}$$

$$= (1-\xi_1)\sqrt{2}\Gamma(\gamma,\beta)\, \kappa_1(\gamma,\beta), \tag{5.64}$$

for an appropriate $\xi_1 \in (0,1)$. Normalizing (5.46) by $\sqrt{n}$ and applying limits, we have

$$\lim_{n\to\infty} \frac{\log M + \log K}{\sqrt{n}} = (1+\xi_2) \left(\lim_{n\to\infty} \sqrt{n}\alpha_n\right) \kappa_2(\gamma,\beta) \tag{5.65}$$

$$= (1+\xi_2)\sqrt{2}\Gamma(\gamma,\beta)\, \kappa_2(\gamma,\beta) \tag{5.66}$$

$$\tag{5.67}$$

where $\xi_2 > 0$, is an appropriate constant.

5.4.2 Proof of converse for Theorem 5

Consider a covert communication scheme for a physically degraded relay channel that satisfies (5.6), (5.7), and (5.8). Let W be the covert message and S be the secret key. Alice and the relay transmit n-length sequences $\mathbf{X}_1 = (X_{11}, X_{12}, \ldots, X_{1n})$ and $\mathbf{X}_2 = (X_{21}, X_{22}, \ldots, X_{2n})$, respectively. For $i \in [\![1, n]\!]$, define the joint distribution of the symbol pair (X_{1i}, X_{2i}) as $\Pi_{X_{1i}X_{2i}}$. We define two random variables $\widetilde{X}_1$ and $\widetilde{X}_2$

with joint distribution $\Pi_{\widetilde{X}_1\widetilde{X}_2}$ defined by

$$\Pi_{\widetilde{X}_1\widetilde{X}_2} \triangleq \frac{1}{n}\sum_{i=1}^{n}\Pi_{X_{1i}X_{2i}}. \tag{5.68}$$

For $a, b \in \{0,1\}$, define $\mu_{ab}^{(n)} \triangleq \Pi_{\widetilde{X}_1\widetilde{X}_2}(a,b)$. We denote the corresponding marginal distributions of $\widetilde{X}_1$ and $\widetilde{X}_2$ by $\Pi_{\widetilde{X}_1}$ and $\Pi_{\widetilde{X}_2}$, respectively. Let $\widehat{P}_{Y_{2i}}$ and $\widehat{P}_{Y_{3i}}$ be the distributions of outputs $\mathbf{Y}_2$ and $\mathbf{Y}_3$, respectively, at bit position $i \in [\![1,n]\!]$. We also define random variables $\widetilde{Y}_2$ and $\widetilde{Y}_3$ with distributions

$$P_{\widetilde{Y}_2}(y_2) = \sum_{x_1,x_2}\Pi_{\widetilde{X}_1\widetilde{X}_2}(x_1,x_2)W_{Y_2|X_1X_2}(y_2|x_1x_2), \tag{5.69}$$

$$P_{\widetilde{Y}_3}(y_3) = \sum_{x_1,x_2}\Pi_{\widetilde{X}_1\widetilde{X}_2}(x_1,x_2)W_{Y_3|X_1X_2}(y_3|x_1x_2), \tag{5.70}$$

respectively. Using standard techniques, we upper bound $\log M$ by

$$\begin{aligned}
\log M &= \mathbb{H}(W) && (5.71)\\
&\overset{(a)}{\leqslant} \mathbb{I}(W;\mathbf{Y}_3) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M && (5.72)\\
&= \sum_{i=1}^{n}\mathbb{I}\big(W;Y_{3i}|\mathbf{Y}_{3,1}^{i-1}\big) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M && (5.73)\\
&= \sum_{i=1}^{n}\Big(\mathbb{H}\big(Y_{3i}|\mathbf{Y}_{3,1}^{i-1}\big) - \mathbb{H}\big(Y_{3i}|W\mathbf{Y}_{3,1}^{i-1}\big)\Big) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M && (5.74)\\
&\leqslant \sum_{i=1}^{n}\Big(\mathbb{H}(Y_{3i}) - \mathbb{H}\big(Y_{3i}|WX_{1i}X_{2i}\mathbf{Y}_{3,1}^{i-1}\big)\Big) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M && (5.75)\\
&\overset{(b)}{=} \sum_{i=1}^{n}\left(\mathbb{H}(Y_{3i}) - \mathbb{H}(Y_{3i}|X_{1i}X_{2i})\right) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M && (5.76)\\
&= \sum_{i=1}^{n}\mathbb{I}(X_{1i}X_{2i};Y_{3i}) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M, && (5.77)
\end{aligned}$$

where (a) follows from Fano's inequality, (b) follows from the fact that Y_{3i} is independent of $(W, \mathbf{Y}_3^{i-1})$ conditioned on (X_{1i}, X_{2i}). Defining a random variable Q uniformly

distributed in $[\![1, n]\!]$, we write write (5.77) as

$$\log M \leqslant n\left(\frac{1}{n}\sum_{i=1}^{n}\mathbb{I}(X_{1Q}X_{2Q}; Y_{3Q}|Q=i)\right) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M \tag{5.78}$$

$$= n\mathbb{I}(X_{1Q}X_{2Q}; Y_{3Q}|Q) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M \tag{5.79}$$

$$= n\left(\mathbb{H}(Y_{3Q}|Q) - \mathbb{H}(Y_{3Q}|X_{1Q}X_{2Q}Q)\right) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M \tag{5.80}$$

$$\leqslant n\left(\mathbb{H}(Y_{3Q}) - \mathbb{H}(Y_{3Q}|X_{1Q}X_{2Q})\right) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M \tag{5.81}$$

$$= n\mathbb{I}(X_{1Q}X_{2Q}; Y_{3Q}) + \mathbb{H}_b\left(\epsilon_n\right) + \epsilon_n \log M. \tag{5.82}$$

Representing (X_{1Q}, X_{2Q}, Y_{3Q}) by $\left(\widetilde{X}_1, \widetilde{X}_2, \widetilde{Y}_3, \right)$ and rearranging the terms in (5.82), we obtain

$$\log M \leqslant \frac{n\mathbb{I}\left(\widetilde{X}_1\widetilde{X}_2; \widetilde{Y}_3\right) + \mathbb{H}_b\left(\epsilon_n\right)}{(1-\epsilon_n)}. \tag{5.83}$$

We upper bound the mutual information term in (5.83) by

$$\mathbb{I}\left(\widetilde{X}_1\widetilde{X}_2; \widetilde{Y}_3\right) = \sum_{x_1}\sum_{x_2}\sum_{y_3}\Pi_{\widetilde{X}_1\widetilde{X}_2}(x_1, x_2)W_{Y_3|X_1X_2}(y_3|x_1x_2)\log\frac{W_{Y_3|X_1X_2}(y_3|x_1x_2)}{P_{\widetilde{Y}_3}(y_3)} \tag{5.84}$$

$$= \mu_{10}^{(n)}\mathbb{D}(P_{10}\|P_{00}) + \mu_{01}^{(n)}\mathbb{D}(P_{01}\|P_{00}) + \mu_{11}^{(n)}\mathbb{D}(P_{11}\|P_{00}) - \mathbb{D}\left(P_{\widetilde{Y}_3}\|P_{00}\right) \tag{5.85}$$

$$\leqslant \mu_{10}^{(n)}\mathbb{D}(P_{10}\|P_{00}) + \mu_{01}^{(n)}\mathbb{D}(P_{01}\|P_{00}) + \mu_{11}^{(n)}\mathbb{D}(P_{11}\|P_{00}). \tag{5.86}$$

Combining (5.83) and (5.86),

$$\log M \leqslant \frac{n\left(\mu_{10}^{(n)}\mathbb{D}(P_{10}\|P_{00}) + \mu_{01}^{(n)}\mathbb{D}(P_{01}\|P_{00}) + \mu_{11}^{(n)}\mathbb{D}(P_{11}\|P_{00})\right) + \mathbb{H}_b\left(\epsilon_n\right)}{(1-\epsilon_n)}. \tag{5.87}$$

Next, we upper bound $\log M$ alternatively by

$$\log M = \mathbb{H}(W) \tag{5.88}$$

$$= \mathbb{I}(W; \mathbf{Y}_2\mathbf{Y}_3) + \mathbb{H}(W|\mathbf{Y}_2\mathbf{Y}_3) \tag{5.89}$$

$$\leqslant \mathbb{I}(W; \mathbf{Y}_2\mathbf{Y}_3) + \mathbb{H}(W|\mathbf{Y}_3) \tag{5.90}$$

$$\leqslant \mathbb{I}(W; \mathbf{Y}_2\mathbf{Y}_3) + \mathbb{H}_b(\epsilon_n) + \epsilon_n \log M \tag{5.91}$$

$$= \sum_{i=1}^{n} \mathbb{I}\big(W; Y_{2i}Y_{3i}|\mathbf{Y}_{2,1}^{i-1}\mathbf{Y}_{3,1}^{i-1}\big) + \mathbb{H}_b(\epsilon_n) + \epsilon_n \log M \tag{5.92}$$

$$= \sum_{i=1}^{n} \Big(\mathbb{H}\big(Y_{2i}Y_{3i}|\mathbf{Y}_{2,1}^{i-1}\mathbf{Y}_{3,1}^{i-1}\big) - \mathbb{H}\big(Y_{2i}Y_{3i}|W\mathbf{Y}_{2,1}^{i-1}\mathbf{Y}_{3,1}^{i-1}\big)\Big) + \mathbb{H}_b(\epsilon_n) + \epsilon_n \log M \tag{5.93}$$

$$\overset{(a)}{=} \sum_{i=1}^{n} \Big(\mathbb{H}\big(Y_{2i}Y_{3i}|X_{2i}\mathbf{Y}_{2,1}^{i-1}\mathbf{Y}_{3,1}^{i-1}\big) - \mathbb{H}\big(Y_{2i}Y_{3i}|W\mathbf{Y}_{2,1}^{i-1}\mathbf{Y}_{3,1}^{i-1}\big)\Big) + \mathbb{H}_b(\epsilon_n) + \epsilon_n \log M \tag{5.94}$$

$$\leqslant \sum_{i=1}^{n} \Big(\mathbb{H}(Y_{2i}Y_{3i}|X_{2i}) - \mathbb{H}\big(Y_{2i}Y_{3i}|WX_{1i}X_{2i}\mathbf{Y}_{2,1}^{i-1}\mathbf{Y}_{3,1}^{i-1}\big)\Big) + \mathbb{H}_b(\epsilon_n) + \epsilon_n \log M \tag{5.95}$$

$$\overset{(b)}{=} \sum_{i=1}^{n} \left(\mathbb{H}(Y_{2i}Y_{3i}|X_{2i}) - \mathbb{H}(Y_{2i}Y_{3i}|X_{1i}X_{2i})\right) + \mathbb{H}_b(\epsilon_n) + \epsilon_n \log M \tag{5.96}$$

$$= \sum_{i=1}^{n} \mathbb{I}(X_{1i}; Y_{2i}Y_{3i}|X_{2i}) + \mathbb{H}_b(\epsilon_n) + \epsilon_n \log M \tag{5.97}$$

$$\overset{(c)}{=} \sum_{i=1}^{n} \mathbb{I}(X_{1i}; Y_{2i}|X_{2i}) + \mathbb{H}_b(\epsilon_n) + \epsilon_n \log M \tag{5.98}$$

$$= n\mathbb{I}(X_{1Q}; Y_{2Q}|X_{2Q}Q) + \mathbb{H}_b(\epsilon_n) + \epsilon_n \log M \tag{5.99}$$

$$= n\left(\mathbb{H}(Y_{2Q}|X_{2Q}Q) - \mathbb{H}(Y_{2Q}|X_{1Q}X_{2Q}Q)\right) + \mathbb{H}_b(\epsilon_n) + \epsilon_n \log M \tag{5.100}$$

$$\leqslant n\left(\mathbb{H}(Y_{2Q}|X_{2Q}) - \mathbb{H}(Y_{2Q}|X_{1Q}X_{2Q})\right) + \mathbb{H}_b(\epsilon_n) + \epsilon_n \log M \tag{5.101}$$

$$= n\mathbb{I}(X_{1Q}; Y_{2Q}|X_{2Q}) + \mathbb{H}_b(\epsilon_n) + \epsilon_n \log M, \tag{5.102}$$

where (a) follows from the fact that X_{2i} is a function of $\mathbf{Y}_{2,1}^{i-1}$, (b) follows from the fact that (Y_{2i}, Y_{3i}) is independent of $\left(W, \mathbf{Y}_{2,1}^{i-1}, \mathbf{Y}_{2,1}^{i-1}\right)$ conditioned on (X_{1i}, X_{2i}), and (c) follows from the fact that $X_1 - (X_2, Y_2) - Y_3$ forms a Markov chain because the relay channel is physically degraded. Representing (X_{1Q}, X_{2Q}, Y_{2Q}) by $\left(\widetilde{X}_1, \widetilde{X}_2, \widetilde{Y}_2\right)$ and rearranging the terms in (5.102), we obtain

$$\log M \leqslant \frac{n\mathbb{I}\left(\widetilde{X}_1; \widetilde{Y}_2 | \widetilde{X}_2\right) + \mathbb{H}_b\left(\epsilon_n\right)}{(1-\epsilon_n)}. \tag{5.103}$$

Expanding the mutual information term in (5.103), we have

$$\mathbb{I}\left(\widetilde{X}_1; \widetilde{Y}_2 | \widetilde{X}_2\right) = \sum_{x_1}\sum_{x_2}\sum_{y_3} \Pi_{\widetilde{X}_1\widetilde{X}_2}(x_1, x_2) W_{Y_2|X_1X_2}(y_2|x_1x_2) \log \frac{W_{Y_2|X_1X_2}(y_2|x_1x_2)}{P_{\widetilde{Y}_2|\widetilde{X}_2}(y_2|x_2)} \tag{5.104}$$

$$\begin{aligned} &= \mu_{10}^{(n)}\mathbb{D}\big(\overline{P}_{10}\|\overline{P}_{00}\big) + \mu_{01}^{(n)}\mathbb{D}\big(\overline{P}_{01}\|\overline{P}_{00}\big) + \mu_{11}^{(n)}\mathbb{D}\big(\overline{P}_{11}\|\overline{P}_{00}\big) \\ &\quad - \left(\mu_{00}^{(n)} + \mu_{10}^{(n)}\right)\mathbb{D}\left(P_{\widetilde{Y}_2|\widetilde{X}_2=0}\|\overline{P}_{00}\right) - \left(\mu_{01}^{(n)} + \mu_{11}^{(n)}\right)\mathbb{D}\left(P_{\widetilde{Y}_2|\widetilde{X}_2=1}\|\overline{P}_{00}\right) \end{aligned} \tag{5.105}$$

$$\begin{aligned} &\leqslant \mu_{10}^{(n)}\mathbb{D}\big(\overline{P}_{10}\|\overline{P}_{00}\big) + \mu_{01}^{(n)}\mathbb{D}\big(\overline{P}_{01}\|\overline{P}_{00}\big) + \mu_{11}^{(n)}\mathbb{D}\big(\overline{P}_{11}\|\overline{P}_{00}\big) \\ &\quad - \left(\mu_{01}^{(n)} + \mu_{11}^{(n)}\right)\mathbb{D}\left(P_{\widetilde{Y}_2|\widetilde{X}_2=1}\|\overline{P}_{00}\right). \end{aligned} \tag{5.106}$$

where $P_{\widetilde{Y}_2|\widetilde{X}_2}(y_2|x_2) \triangleq \sum_{x_1} \Pi_{\widetilde{X}_1}(x_1) W_{Y_2|X_1X_2}(y_2|x_1x_2)$. Combining (5.103) and (5.106), we have

$$\begin{aligned} \log M \leqslant \frac{n}{(1-\epsilon_n)} &\Big(\mu_{10}^{(n)}\mathbb{D}\big(\overline{P}_{10}\|\overline{P}_{00}\big) + \mu_{01}^{(n)}\mathbb{D}\big(\overline{P}_{01}\|\overline{P}_{00}\big) + \mu_{11}^{(n)}\mathbb{D}\big(\overline{P}_{11}\|\overline{P}_{00}\big) \\ &- \left(\mu_{01}^{(n)} + \mu_{11}^{(n)}\right)\mathbb{D}\left(P_{\widetilde{Y}_2|\widetilde{X}_2=1}\|\overline{P}_{00}\right)\Big) + \frac{\mathbb{H}_b\left(\epsilon_n\right)}{(1-\epsilon_n)}. \end{aligned} \tag{5.107}$$

Let $\widehat{Q}_1^n$ and $\widehat{Q}_2^n$ be the distributions of observations $\mathbf{Z}_1$ and $\mathbf{Z}_2$, respectively, at

the wardens. We lower bound the KL divergence between $\widehat{Q}_1^n$ and $Q_0^{\otimes n}$ by

$$\mathbb{D}\Big(\widehat{Q}_1^n \| Q_0^{\otimes n}\Big) = -\mathbb{H}(\mathbf{Z}_1) + \mathbb{E}_{\widehat{Q}_1^n}\left(\log \frac{1}{Q_0^{\otimes n}(\mathbf{Z}_1)}\right) \tag{5.108}$$

$$\geqslant \sum_{i=1}^{n}\left(-\mathbb{H}(Z_{1i}) + \mathbb{E}_{\widehat{Q}_{1i}}\left(\log \frac{1}{Q_0(Z_{1i})}\right)\right) \tag{5.109}$$

$$= \sum_{i=1}^{n} \mathbb{D}\Big(\widehat{Q}_{1i} \| Q_0\Big) \tag{5.110}$$

$$\geqslant n\mathbb{D}\big(Q_{\widetilde{Z}_1} \| Q_0\big), \tag{5.111}$$

where $Q_{\widetilde{Z}_1}(z_1) \triangleq \sum_{x_1} \Pi_{\widetilde{X}_1}(x_1) W_{Z_1|X_1}(z_1|x_1)$. From (5.7), we have

$$\delta_1 \geqslant \limsup_{n\to\infty} \mathbb{D}\Big(\widehat{Q}_1^n \| Q_0^{\otimes n}\Big) \geqslant \limsup_{n\to\infty} n\mathbb{D}\big(Q_{\widetilde{Z}_1} \| Q_0\big). \tag{5.112}$$

Since δ_1 does not grow with n, we have

$$\limsup_{n\to\infty} \mathbb{D}\big(Q_{\widetilde{Z}_1} \| Q_0\big) = 0. \tag{5.113}$$

Then, by Pinsker's inequality, we have $\limsup_{n\to\infty} \mathbb{V}\big(Q_{\widetilde{Z}_1}, Q_0\big) = 0$. For every $z_1 \in \mathcal{Z}_1$, we have

$$\limsup_{n\to\infty} Q_{\widetilde{Z}_1}(z_1) = Q_0(z_1) \tag{5.114}$$

$$\limsup_{n\to\infty} \big(\Pi_{\widetilde{X}_1}(1) Q_1(z_1) + \Pi_{\widetilde{X}_1}(0) Q_0(z_1)\big) = Q_0(z_1) \tag{5.115}$$

$$\left(\limsup_{n\to\infty} \Pi_{\widetilde{X}_1}(1)\right)\big(Q_1(z_1) - Q_0(z_1)\big) = 0. \tag{5.116}$$

Since $Q_1(z_1) \neq Q_0(z_1)$, for all $z_1 \in \mathcal{Z}_1$ and since $\widetilde{\Pi}_{X_1}(1)$ is non-negative, we conclude

from (5.116) that

$$\lim_{n\to\infty} \Pi_{\widetilde{X}_1}(1) = 0 \tag{5.117}$$

$$\lim_{n\to\infty} \left(\mu_{10}^{(n)} + \mu_{11}^{(n)}\right) = 0. \tag{5.118}$$

Defining $\widetilde{Q}_{Z_2}(z_2) \triangleq \sum_{x_2} \Pi_{\widetilde{X}_2}(x_2) W_{Z_2|X_2}(z_2|x_2)$ and using similar steps, we obtain

$$\mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_0^{\otimes n}\Big) \geqslant n\mathbb{D}\big(Q_{\widetilde{Z}_2} \| \overline{Q}_0\big). \tag{5.119}$$

Then, from (5.119), we have

$$\limsup_{n\to\infty} \mathbb{D}\big(Q_{\widetilde{Z}_2} \| \overline{Q}_0\big) = 0. \tag{5.120}$$

Using Pinsker's inequality, we have $\limsup_{n\to\infty} \mathbb{V}\big(Q_{\widetilde{Z}_2}, \overline{Q}_0\big) = 0$. Consequently, using similar steps as we used to obtain (5.116) and (5.118), we have

$$\lim_{n\to\infty} \Pi_{\widetilde{X}_2}(1) = \lim_{n\to\infty} \left(\mu_{01}^{(n)} + \mu_{11}^{(n)}\right) = 0. \tag{5.121}$$

Combining (5.118) and (5.121), we conclude that, for $(a,b) \in \{0,1\}^2 \setminus (0,0)$,

$$\lim_{n\to\infty} \mu_{ab}^{(n)} = 0. \tag{5.122}$$

We define

$$\Psi_1^{(n)}(z_1) \triangleq \Pi_{\widetilde{X}_1}(1) \left(Q_1(z_1) - Q_0(z_1)\right), \tag{5.123}$$

$$\xi_1^{(n)}(z_1) \triangleq \frac{\Psi_1^{(n)}(z_1)}{Q_0(z_1)} + \frac{4\left|\Psi_1^{(n)}(z_1)\right|}{3Q_0(z_1)}. \tag{5.124}$$

We lower bound (5.111) by

$$\mathbb{D}\Big(\widehat{Q}_1^n \| Q_0^{\otimes n}\Big) \geqslant n\mathbb{D}\big(Q_{\widetilde{Z}_1} \| Q_0\big) \tag{5.125}$$

$$= n \sum_{z_1} Q_{\widetilde{Z}_1}(z_1) \log \frac{Q_{\widetilde{Z}_1}(z_1)}{Q_0(z_1)} \tag{5.126}$$

$$= n \sum_{z_1} Q_0(z_1) \left(1 + \Pi_{\widetilde{X}_1}(1) \left(\frac{Q_1(z_1) - Q_0(z_1)}{Q_0(z_1)}\right)\right) \times \log \left(1 + \Pi_{\widetilde{X}_1}(1) \left(\frac{Q_1(z_1) - Q_0(z_1)}{Q_0(z_1)}\right)\right) \tag{5.127}$$

$$= n \sum_{z_1} Q_0(z_1) \left(1 + \frac{\Psi_1^{(n)}(z_1)}{Q_0(z_1)}\right) \log \left(1 + \frac{\Psi_1^{(n)}(z_1)}{Q_0(z_1)}\right) \tag{5.128}$$

$$\overset{(a)}{\geqslant} n \sum_{z_1} \left(\frac{\left(\Psi_1^{(n)}(z_1)\right)^2}{2Q_0(z_1)} - \frac{\left(\Psi_1^{(n)}(z_1)\right)^3}{2Q_0^2(z_1)} \right) + n \sum_{z_1 : \Psi_1^{(n)}(z_1) < 0} \frac{2\left(\Psi_1^{(n)}(z_1)\right)^3}{3Q_0^2(z_1)} \tag{5.129}$$

$$\geqslant n \sum_{z_1} \left(\frac{\left(\Psi_1^{(n)}(z_1)\right)^2}{2Q_0(z_1)} \right) \left(1 - \xi_1^{(n)}(z_1)\right) \tag{5.130}$$

$$\geqslant \sum_{z_1} \left(1 - \xi_1^{(n)}(z_1)\right) n \left(\mu_{10}^{(n)} + \mu_{11}^{(n)}\right)^2 \frac{\left(Q_1(z_1) - Q_0(z_1)\right)^2}{2Q_0(z_1)}, \tag{5.131}$$

where (a) follows from the inequality $\log(1+x) \geqslant x - \frac{x^2}{2}$ for $x \geqslant 0$ and $\log(1+x) \geqslant x - \frac{x^2}{2} + \frac{2x^3}{3}$ for $x \in \Big[-\frac{1}{2}, 0\Big)$. Also, define

$$\Psi_2^{(n)}(z_2) \triangleq \Pi_{\widetilde{X}_2}(1) \left(\overline{Q}_1(z_2) - \overline{Q}_0(z_2)\right), \tag{5.132}$$

$$\xi_2^{(n)}(z_2) \triangleq \frac{\Psi_2^{(n)}(z_2)}{\overline{Q}_0(z_2)} + \frac{4\left|\Psi_2^{(n)}(z_2)\right|}{3\overline{Q}_0(z_2)}. \tag{5.133}$$

By following similar steps, we lower bound (5.119) by

$$\mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_0^{\otimes n}\Big) \geqslant \sum_{z_2} \left(1 - \xi_2^{(n)}(z_2)\right) n \left(\mu_{01}^{(n)} + \mu_{11}^{(n)}\right)^2 \frac{\left(Q_1(z_2) - \overline{Q}_0(z_2)\right)^2}{2\overline{Q}_0(z_2)}. \tag{5.134}$$

Using (5.7), (5.8), (5.131) and (5.134), we obtain

$$\delta_1 \geqslant \limsup_{n\to\infty} \frac{n\left(\mu_{10}^{(n)}+\mu_{11}^{(n)}\right)^2}{2}\chi_2, \tag{5.135}$$

$$\delta_2 \geqslant \limsup_{n\to\infty} \frac{n\left(\mu_{01}^{(n)}+\mu_{11}^{(n)}\right)^2}{2}\overline{\chi}_2. \tag{5.136}$$

For $n \in \mathbb{N}^*$, define $\beta_n \triangleq \frac{\mu_{11}^{(n)}}{\mu_{01}^{(n)}+\mu_{11}^{(n)}}$ and $\gamma_n = \frac{\mu_{01}^{(n)}+\mu_{11}^{(n)}}{\mu_{10}^{(n)}}$. Note that the last KL divergence term in (5.107) can be written as

$$\mathbb{D}\Big(P_{\widetilde{Y}_2|\widetilde{X}_2=1}\|\overline{P}_{00}\Big) = \mathbb{D}\big((1-\beta_n)\overline{P}_{01}+\beta_n\overline{P}_{11}\|\overline{P}_{00}\big). \tag{5.137}$$

Combining (5.87) and (5.107), we have

$$\log M \leqslant \frac{n\mu_{10}^{(n)}\kappa_1\left(\gamma_n,\beta_n\right)}{1-\epsilon_n} + \frac{\mathbb{H}_b\left(\epsilon_n\right)}{1-\epsilon_n}. \tag{5.138}$$

For any $\eta > 0$, (5.135) and (5.136) imply that, for an n large enough,

$$\sqrt{n}\mu_{10}^{(n)} \leq (1+\eta)\sqrt{2}\Gamma(\gamma_n,\beta_n). \tag{5.139}$$

Combining (5.138) and (5.139), and letting $\eta \downarrow 0$ proves the converse part of (5.16).

Next, we lower bound $\log MK$. Note that, if a sequence of codes achieves the limit in (5.16), then it must contain a subsequence satisfying $\gamma_n \to \gamma^*$, $\beta_n \to \beta^*$, and $\sqrt{n}\mu_{10}^{(n)} \to \sqrt{2}\Gamma(\gamma^*,\beta^*)$ as $n \to \infty$, for some (γ^*,β^*) that achieves the limit on the

right-hand side of (5.16). For any code in this subsequence, we have

$$\log MK \geqslant \mathbb{I}(\mathbf{X}_1; \mathbf{Z}_1) \tag{5.140}$$

$$= n \sum_x \sum_z \Pi_{\widetilde{X}_1}(x) W_{Z_1|X_1}(z|x) \log \frac{W_{Z_1|X_1}(z|x)}{Q_0(z)} - \mathbb{D}\Big(\widehat{Q}_1^n \| Q_0^{\otimes n}\Big) \tag{5.141}$$

$$= n\mu_{10}^{(n)} \left(1 + \gamma_n \beta_n\right) \mathbb{D}(Q_1 \| Q_0) - \mathbb{D}\Big(\widehat{Q}_1^n \| Q_0^{\otimes n}\Big), \tag{5.142}$$

and, similarly,

$$\log MK \geqslant n\mu_{10}^{(n)} \gamma_n \mathbb{D}\big(\overline{Q}_1 \| \overline{Q}_0\big) - \mathbb{D}\Big(\widehat{Q}_2^n \| \overline{Q}_0^{\otimes n}\Big). \tag{5.143}$$

Normalizing (5.142) and (5.143) by $\sqrt{n}$ and applying the limits, we have (for the entire sequence of codes)

$$\liminf_{n\to\infty} \frac{\log MK}{\sqrt{n}} \geqslant \sqrt{2}\Gamma(\gamma^*, \beta^*) \kappa_2\left(\gamma^*, \beta^*\right). \tag{5.144}$$

Combining (5.16) and (5.144) proves that $\log K$ must satisfy (5.18).

APPENDIX

5.A Proof of Lemma 12

The decoding error probability averaged over all random codebooks is

$$\begin{aligned}
\mathbb{E}_{\mathcal{C}}\left(P_e\right) &\triangleq \mathbb{E}_{\mathcal{C}}\left(\mathbb{P}\left(\widehat{W} \neq W\right)\right) && (5.145)\\
&= \mathbb{E}_{\mathcal{C}}\left(\mathbb{P}\left(\bigcup_{b=1}^{B+1} \text{Error in block } b\right)\right) && (5.146)\\
&= \sum_{b=1}^{B+1} \mathbb{E}_{\mathcal{C}}\left(\mathbb{P}(\text{Error in block } b|\text{No errors in all previous blocks})\right) && (5.147)\\
&= \sum_{b=1}^{B+1} \mathbb{E}_{\mathcal{C}}\left(P_{e,b}\right) && (5.148)
\end{aligned}$$

where $P_{e,b} \triangleq \mathbb{P}(\text{Error in block } b|\text{No errors in all previous blocks})$. Splitting $P_{e,b}$ between the error probabilities at the relay and Bob using the union bound, we get

$$\begin{aligned}
\mathbb{E}_{\mathcal{C}}\left(P_{e,b}\right) &= \mathbb{E}_{\mathcal{C}}\left(\mathbb{P}(\text{Error in block } b|\text{No errors in previous blocks})\right) && (5.149)\\
&\leqslant \mathbb{E}_{\mathcal{C}}\left(\mathbb{P}(\text{Error in block } b \text{ at the relay}|\text{No errors in previous blocks})\right)\\
&\quad + \mathbb{E}_{\mathcal{C}}\left(\mathbb{P}(\text{Error in block } b \text{ at Bob}|\text{No errors in previous blocks})\right) && (5.150)\\
&\triangleq \mathbb{E}_{\mathcal{C}}\left(P_{e,b}^{(1)}\right) + \mathbb{E}_{\mathcal{C}}\left(P_{e,b}^{(2)}\right). && (5.151)
\end{aligned}$$

For $(m, m') \in [\![1, M']\!]^2$ and $(k, k') \in [\![1, K']\!]$ define the following events

$$\begin{aligned}
E_{2b,(k,k')}(m,m') &\triangleq \left\{\left(\mathbf{X}_{1b,(k,k')}(m,m'), \mathbf{X}_{2b,k}(m), \mathbf{Y}_{2b}\right) \in \mathcal{A}_{\eta_1}^N\right\}, && (5.152)\\
E_{3b,(k,k')}(m,m') &\triangleq \left\{\left(\mathbf{X}_{1b,(k,k')}(m,m'), \mathbf{X}_{2b,k}(m), \mathbf{Y}_{3b}\right) \in \mathcal{A}_{\eta_{21}}^N\right\}, && (5.153)\\
E_{3b,k}(m) &\triangleq \left\{\left(\mathbf{X}_{2b,k}(m), \mathbf{Y}_{3b}\right) \in \mathcal{A}_{\eta_{22}}^N\right\}, && (5.154)
\end{aligned}$$

$$\widetilde{E}_{3b,(k,k')}(m,m') \triangleq E_{3(b-1),(k,k')}(m,m') \cap E_{3b,k}(m). \tag{5.155}$$

Denoting (k_{b-1}, k_b) by (i,j), respectively, we upper bound the first term in (5.151) by

$$\begin{aligned}
\mathbb{E}_{\mathcal{C}}\left(P_{e,b}^{(1)}\right) &\overset{(a)}{=} \mathbb{E}_{\mathcal{C}}\left(\sum_{\mathbf{y}_{2b}} \frac{1}{(M')^2} \sum_{m,m'} W_{Y_2|X_1X_2}^{\otimes N}\left(\mathbf{y}_{2b}|\mathbf{X}_{1b,(i,j)}(m,m')\mathbf{X}_{2b,i}(m)\right)\right. \\
&\qquad \left. \times \mathbb{1}\left\{\bigcup_{\ell \neq m'} E_{2b,(i,j)}(m,\ell) \cup E_{2b,(i,j)}^c(m,m')\right\}\right) \qquad (5.156) \\
&\overset{(b)}{\leqslant} \sum_{\mathbf{y}_{2b}} \sum_{\ell \neq 1} \sum_{\mathbf{x}_{1b,(i,j)}(1,\ell)} \sum_{\mathbf{x}_{2b,i}(1)} P_{Y_2|X_2}^{\otimes N}\left(\mathbf{y}_{2b}|\mathbf{x}_{2b,i}(1)\right) \Pi_{X_2}^{\otimes N}\left(\mathbf{x}_{2b,i}(1)\right) \\
&\qquad \times \Pi_{X_1|X_2}^{\otimes N}\left(\mathbf{x}_{1b,(i,j)}(1,\ell)|\mathbf{x}_{2b,i}(1)\right) \mathbb{1}\left\{\left(\mathbf{x}_{1b,(i,j)}(1,\ell), \mathbf{x}_{2b,i}(1), \mathbf{y}_{2b}\right) \in \mathcal{A}_{\eta_1}^N\right\} \\
&\qquad + \sum_{\mathbf{y}_{2b}} \sum_{\mathbf{x}_{1b,(i,j)}(1,1)} \sum_{\mathbf{x}_{2b,i}(1)} W_{Y_2|X_1X_2}^{\otimes N}\left(\mathbf{y}_{2b}|\mathbf{x}_{1b,(i,j)}(1,1)\mathbf{x}_{2b,i}(1)\right) \\
&\qquad \times \Pi_{X_1X_2}^{\otimes N}\left(\mathbf{x}_{1b,(i,j)}(1,1), \mathbf{x}_{2b,i}(1)\right) \mathbb{1}\left\{\left(\mathbf{x}_{1b,(i,j)}(1,1), \mathbf{x}_{2b,i}(1), \mathbf{y}_{2b}\right) \notin \mathcal{A}_{\eta_1}^N\right\} \qquad (5.157) \\
&\leqslant M' e^{-\eta_1} \sum_{\mathbf{y}_{2b}} \sum_{\mathbf{x}_{1b}} \sum_{\mathbf{x}_{2b}} W_{Y_2|X_1X_2}^{\otimes N}\left(\mathbf{y}_{2b}|\mathbf{x}_{1b}\mathbf{x}_{2b}\right) \Pi_{X_1X_2}^{\otimes N}\left(\mathbf{x}_{1b}, \mathbf{x}_{2b}\right) + \mathbb{P}\left(\mathcal{A}_{\eta_1}^{N\,c}\right) \qquad (5.158) \\
&= M' e^{-\eta_1} + \mathbb{P}\left(\mathcal{A}_{\eta_1}^{N\,c}\right). \qquad (5.159)
\end{aligned}$$

where (a) follows from the fact that there is no error in m since $P_{e,b}^{(1)}$ is the error probability in block b at the relay conditioned on no errors in all previous blocks, and (b) follows from the union bound. Denoting (k_{b-2}, k_{b-1}, k_b) by (i,j,k) and defining

$\eta_2 \triangleq \eta_{21} + \eta_{22}$, we upper bound the second term in (5.151).

$$
\begin{aligned}
&\mathbb{E}_{\mathcal{C}}\left(P_{e,b}^{(2)}\right) \\
&\quad \overset{(a)}{=} \mathbb{E}_{\mathcal{C}}\Bigg(\sum_{\mathbf{y}_{3(b-1)}} \sum_{\mathbf{y}_{3b}} \frac{1}{(M')^3} \sum_{m,m',m''} W_{Y_3|X_1X_2}^{\otimes N}\left(\mathbf{y}_{3(b-1)}|\mathbf{X}_{1(b-1),(i,j)}(m,m')\mathbf{X}_{2(b-1),i}(m)\right) \\
&\qquad \times W_{Y_3|X_1X_2}^{\otimes N}\left(\mathbf{y}_{3b}|\mathbf{X}_{1b,(j,k)}(m',m''),\mathbf{X}_{2b,j}(m')\right) \\
&\qquad \times \mathbb{1}\left\{ \bigcup_{\ell \neq m'} \widetilde{E}_{3b,(i,j)}(m,\ell) \cup \widetilde{E}_{3b,(i,j)}^{c}(m,m') \right\} \Bigg) \qquad (5.160) \\
&\quad \leqslant \sum_{\mathbf{y}_{3(b-1)}} \sum_{\mathbf{y}_{3b}} \sum_{\ell \neq 1} \sum_{\mathbf{x}_{2(b-1),i}(1)} \sum_{\mathbf{x}_{1(b-1),(i,j)}(1,\ell)} \sum_{\mathbf{x}_{2b,j}(\ell)} P_{Y_3|X_2}^{\otimes N}\left(\mathbf{y}_{3(b-1)}|\mathbf{x}_{2(b-1),i}(1)\right) \\
&\qquad \times \Pi_{X_1X_2}^{\otimes N}\left(\mathbf{x}_{1(b-1),(i,j)}(1,\ell),\mathbf{x}_{2(b-1),i}(1)\right) P_{Y_3}^{\otimes N}\left(\mathbf{y}_{3b}\right) \Pi_{X_2}^{\otimes N}\left(\mathbf{x}_{2b,j}(\ell)\right) \\
&\qquad \times \mathbb{1}\left\{\left(\mathbf{x}_{1(b-1),(i,j)}(1,\ell),\mathbf{x}_{2(b-1),i}(1),\mathbf{y}_{3(b-1)}\right) \in \mathcal{A}_{\eta_{21}}^{N}\right\} \mathbb{1}\left\{\left(\mathbf{x}_{2b,j}(\ell),\mathbf{y}_{3b}\right) \in \mathcal{A}_{\eta_{22}}^{N}\right\} \\
&\qquad + \sum_{\mathbf{y}_{3(b-1)}} \sum_{\mathbf{y}_{3b}} \sum_{\mathbf{x}_{1(b-1),(i,j)}(1,1)} \sum_{\mathbf{x}_{2(b-1),i}(1)} \sum_{\mathbf{x}_{2b,j}(1)} 1 \\
&\qquad \times W_{Y_3|X_1X_2}^{\otimes N}\left(\mathbf{y}_{3(b-1)}|\mathbf{x}_{1(b-1),(i,j)}(1,1)\mathbf{x}_{2(b-1),i}(1)\right) P_{Y_3|X_2}^{\otimes N}\left(\mathbf{y}_{3b}|\mathbf{x}_{2b,j}(1)\right) \\
&\qquad \times \Pi_{X_1X_2}^{\otimes N}\left(\mathbf{x}_{1(b-1),(i,j)}(1,1),\mathbf{x}_{2(b-1),i}(1)\right) \Pi_{X_2}^{\otimes N}\left(\mathbf{x}_{2b,j}(1)\right) \\
&\qquad \times \left(\mathbb{1}\left\{\left(\mathbf{x}_{1(b-1),(i,j)}(1,1),\mathbf{x}_{2(b-1),i}(1),\mathbf{y}_{3b}\right) \notin \mathcal{A}_{\eta_{21}}^{N}\right\} + \mathbb{1}\left\{\left(\mathbf{x}_{2b,j}(1),\mathbf{y}_{3b}\right) \notin \mathcal{A}_{\eta_{22}}^{N}\right\}\right) \qquad (5.161) \\
&\quad \leqslant M' e^{-(\eta_{21}+\eta_{22})} \sum_{\mathbf{y}_{3(b-1)}} \sum_{\mathbf{x}_{1(b-1)}} \sum_{\mathbf{x}_{2(b-1)}} \sum_{\mathbf{y}_{3b}} \sum_{\mathbf{x}_{2b}} W_{Y_3|X_1X_2}^{\otimes N}\left(\mathbf{y}_{3(b-1)}|\mathbf{x}_{1(b-1)}\mathbf{x}_{2(b-1)}\right) \\
&\qquad \times \Pi_{X_1X_2}^{\otimes N}\left(\mathbf{x}_{1(b-1)},\mathbf{x}_{2(b-1)}\right) P_{Y_3|X_2}^{\otimes N}\left(\mathbf{y}_{3b}|\mathbf{x}_{2b}\right) \Pi_{X_2}^{\otimes N}\left(\mathbf{x}_{2b}\right) + \mathbb{P}\left(\mathcal{A}_{\eta_{21}}^{N\ c}\right) + \mathbb{P}\left(\mathcal{A}_{\eta_{22}}^{N\ c}\right) \qquad (5.162) \\
&\quad = M' e^{-\eta_2} + \mathbb{P}\left(\mathcal{A}_{\eta_{21}}^{N\ c}\right) + \mathbb{P}\left(\mathcal{A}_{\eta_{22}}^{N\ c}\right). \qquad (5.163)
\end{aligned}
$$

where (a) follows from the fact that there are no errors in m since $P_{e,b}^{(2)}$ is the error probability in block b at Bob conditioned on no errors in all previous blocks. Error in m'', if any, will be part of the error analysis of $P_{e,b+1}^{(2)}$. Combining (5.151), (5.159),

and (5.163), we obtain

$$\mathbb{E}_{\mathcal{C}}\left(P_{e,b}\right) \leqslant M' e^{-\eta_1} + M' e^{-\eta_2} + \mathbb{P}\big(\mathcal{A}_{\eta_1}^{N\,c}\big) + \mathbb{P}\big(\mathcal{A}_{\eta_{21}}^{N\ \ c}\big) + \mathbb{P}\big(\mathcal{A}_{\eta_{22}}^{N\ \ c}\big). \tag{5.164}$$

For an arbitrary $\mu \in (0,1)$, we define

$$\eta_1 \triangleq (1-\mu)\, N\mathbb{I}(X_1; Y_2|X_2), \tag{5.165}$$

$$\eta_{21} \triangleq (1-\mu)\, N\mathbb{I}(X_1; Y_3|X_2), \tag{5.166}$$

$$\eta_{22} \triangleq (1-\mu)\, N\mathbb{I}(X_2; Y_3). \tag{5.167}$$

From the definition of η_2, we have

$$\eta_2 = (1-\mu)\, N\mathbb{I}(X_1X_2; Y_3). \tag{5.168}$$

Expanding the mutual information term in (5.165), we obtain

$$\mathbb{I}(X_1; Y_2|X_2) = (1-\gamma\alpha_n)\, \mathbb{I}(X_1; Y_2|X_2=0) + \gamma\alpha_n \mathbb{I}(X_1; Y_2|X_2=1). \tag{5.169}$$

We expand the two mutual information terms on the right hand side of (5.169) as follows.

$$\mathbb{I}(X_1; Y_2|X_2=0) = \alpha_n \mathbb{D}\big(\overline{P}_{10} \| \overline{P}_{00}\big) - \mathbb{D}\big(W_{Y_2|X_2=0} \| \overline{P}_{00}\big), \tag{5.170}$$

$$\mathbb{I}(X_1; Y_2|X_2=1) = (1-\beta)\, \mathbb{D}\big(\overline{P}_{01} \| \overline{P}_{00}\big) + \beta \mathbb{D}\big(\overline{P}_{11} \| \overline{P}_{00}\big) - \mathbb{D}\big(W_{Y_2|X_2=1} \| \overline{P}_{00}\big). \tag{5.171}$$

Note that we can write $W_{Y_2|X_2}(y_2|0) = \overline{P}_{00}(y_2) + \alpha_n \big(\overline{P}_{10}(y_2) - \overline{P}_{00}(y_2)\big)$. Then, we rewrite the last KL divergence term on the right hand side of (5.170) as

$$\begin{aligned}
\mathbb{D}\big(W_{Y_2|X_2=0}\|\overline{P}_{00}\big) &= \sum_{y_2} W_{Y_2|X_2}(y_2|0) \log \frac{W_{Y_2|X_2}(y_2|0)}{\overline{P}_{00}(y_2)} && (5.172)\\
&= \sum_{y_2} \overline{P}_{00}(y_2) \left(1 + \alpha_n \frac{\overline{P}_{10}(y_2) - \overline{P}_{00}(y_2)}{\overline{P}_{00}(y_2)}\right) \\
&\quad \times \log \left(1 + \alpha_n \frac{\overline{P}_{10}(y_2) - \overline{P}_{00}(y_2)}{\overline{P}_{00}(y_2)}\right) && (5.173)\\
&\overset{(a)}{=} \mathcal{O}\left(\alpha_n^2\right), && (5.174)
\end{aligned}$$

where (a) follows from the Taylor series expansion of the log term. Moreover, the last KL divergence term on the right hand side of (5.171) can be expanded as

$$\mathbb{D}\big(W_{Y_2|X_2=1}\|\overline{P}_{00}\big) = \mathbb{D}\big((1-\beta)\overline{P}_{01} + \beta\overline{P}_{11}\|\overline{P}_{00}\big). \tag{5.175}$$

Combining (5.169), (5.170), (5.171), and (5.174), we have

$$\begin{aligned}
\mathbb{I}(X_1; Y_2|X_2) &= \alpha_n \left(\mathbb{D}\big(\overline{P}_{10}\|\overline{P}_{00}\big) + \gamma(1-\beta)\mathbb{D}\big(\overline{P}_{01}\|\overline{P}_{00}\big) + \gamma\beta\mathbb{D}\big(\overline{P}_{11}\|\overline{P}_{00}\big)\right) \\
&\quad - \alpha_n\gamma\mathbb{D}\big((1-\beta)\overline{P}_{01} + \beta\overline{P}_{11}\|\overline{P}_{00}\big) + \mathcal{O}\left(\alpha_n^2\right). && (5.176)
\end{aligned}$$

Next, we expand the mutual information term in (5.168) as

$$\begin{aligned}
\mathbb{I}(X_1X_2; Y_3) &= \alpha_n \left(\mathbb{D}(P_{10}\|P_{00}) + \gamma(1-\beta)\mathbb{D}(P_{01}\|P_{00}) + \gamma\beta\mathbb{D}(P_{11}\|P_{00})\right) \\
&\quad - \mathbb{D}(P_{Y_3}\|P_{00}) + \mathcal{O}\left(\alpha_n^2\right). && (5.177)
\end{aligned}$$

We define

$$L(y_3) \triangleq \gamma\beta\left(P_{11}(y_3) - P_{01}(y_3)\right) + \gamma\left(P_{01}(y_3) - P_{00}(y_3)\right) + \left(1 - \gamma\alpha_n\right)\left(P_{10}(y_3) - P_{00}(y_3)\right). \tag{5.178}$$

Using (5.178), we write

$$P_{Y_3}(y_3) = P_{00}(y_3) + \alpha_n L(y_3). \tag{5.179}$$

The last KL divergence term on the right hand side of (5.177) can be written as

$$\begin{aligned}
\mathbb{D}(P_{Y_3}\|P_{00}) &= \sum_{y_3} P_{Y_3}(y_3)\log\frac{P_{Y_3}(y_3)}{P_{00}(y_3)} && (5.180)\\
&= \sum_{y_3} P_{00}(y_3)\left(1+\alpha_n\frac{L(y_3)}{P_{00}(y_3)}\right)\log\left(1+\alpha_n\frac{L(y_3)}{P_{00}(y_3)}\right) && (5.181)\\
&\overset{(a)}{=} \mathcal{O}\left(\alpha_n^2\right), && (5.182)
\end{aligned}$$

where, (a) follows from the expansion of the log term using Taylor series and the fact that $\sum_{y_3} L(y_3) = 0$. Combining (5.177) and (5.182), we have

$$\mathbb{I}(X_1X_2;Y_3) = \alpha_n\left(\mathbb{D}(P_{10}\|P_{00}) + \gamma(1-\beta)\mathbb{D}(P_{01}\|P_{00}) + \gamma\beta\mathbb{D}(P_{11}\|P_{00})\right) + \mathcal{O}\left(\alpha_n^2\right). \tag{5.183}$$

Using (5.176) and (5.183), we rewrite (5.165) and (5.168) as

$$\begin{aligned}
\eta_1 &= (1-\mu)N\alpha_n\left(\mathbb{D}\big(\overline{P}_{10}\|\overline{P}_{00}\big) + \gamma(1-\beta)\mathbb{D}\big(\overline{P}_{01}\|\overline{P}_{00}\big) + \gamma\beta\mathbb{D}\big(\overline{P}_{11}\|\overline{P}_{00}\big)\right)\\
&\quad - (1-\mu)N\alpha_n\gamma\mathbb{D}\big((1-\beta)\overline{P}_{01} + \beta\overline{P}_{11}\|\overline{P}_{00}\big) + N\mathcal{O}\left(\alpha_n^2\right), && (5.184)\\
\eta_2 &= (1-\mu)N\alpha_n\left(\mathbb{D}(P_{10}\|P_{00}) + \gamma(1-\beta)\mathbb{D}(P_{01}\|P_{00}) + \gamma\beta\mathbb{D}(P_{11}\|P_{00})\right) + N\mathcal{O}\left(\alpha_n^2\right). && (5.185)
\end{aligned}$$

Using Bernstein's inequality, we can upper bound the last three terms in (5.164) by

$$\mathbb{P}\big(\mathcal{A}_{\eta_1}^{N\,c}\big) + \mathbb{P}\big(\mathcal{A}_{\eta_{21}}^{N\ c}\big) + \mathbb{P}\big(\mathcal{A}_{\eta_{22}}^{N\ c}\big) \leqslant \exp\left(-a_1 n\alpha_n\right), \tag{5.186}$$

for an appropriate constant $a_1 > 0$. For a large n, if we choose M' such that

$$\begin{aligned}\log M' < (1-\mu)\, N\alpha_n \left(\mathbb{D}\big(\overline{P}_{10}\|\overline{P}_{00}\big) + \gamma(1-\beta)\mathbb{D}\big(\overline{P}_{01}\|\overline{P}_{00}\big) + \gamma\beta\mathbb{D}\big(\overline{P}_{11}\|\overline{P}_{00}\big)\right) \\ - (1-\mu)\, N\alpha_n\gamma\mathbb{D}\big((1-\beta)\overline{P}_{01} + \beta\overline{P}_{11}\|\overline{P}_{00}\big),\end{aligned} \tag{5.187}$$

$$\log M' < (1-\mu)\, N\alpha_n \left(\mathbb{D}(P_{10}\|P_{00}) + \gamma(1-\beta)\mathbb{D}(P_{01}\|P_{00}) + \gamma\beta\mathbb{D}(P_{11}\|P_{00})\right), \tag{5.188}$$

the error probability averaged over all random codebooks $\mathcal{C}$ can be upper bounded by

$$\begin{aligned}\mathbb{E}_{\mathcal{C}}\left(P_e\right) &\leqslant \sum_{b=1}^{B+1} \exp\left(-a_2 n\alpha_n\right) &(5.189)\\ &\leqslant \exp\left(-a_3 n\alpha_n\right), &(5.190)\end{aligned}$$

for appropriate constants $a_2, a_3 > 0$.

5.B Proof of Lemma 13

Define the sets

$$\mathcal{B}_{\tau_1}^N \triangleq \left\{(\mathbf{x}_1, \mathbf{z}_1) \in \mathcal{X}^N \times \mathcal{Z}_1^N : \log \frac{W_{Z_1|X_1}^{\otimes N}(\mathbf{z}_1|\mathbf{x}_1)}{Q_{\alpha_n}^{\otimes N}(\mathbf{z}_1)} < \tau_1\right\}, \tag{5.191}$$

$$\mathcal{B}_{\tau_2}^N \triangleq \left\{(\mathbf{x}_2, \mathbf{z}_2) \in \mathcal{X}^N \times \mathcal{Z}_2^N : \log \frac{W_{Z_2|X_2}^{\otimes N}(\mathbf{z}_2|\mathbf{x}_2)}{Q_{\alpha_n}^{\otimes N}(\mathbf{z}_2)} < \tau_2\right\}, \tag{5.192}$$

where τ_1 and τ_2 will be defined later. Let the sequence $\mathbf{z}_1$ be a concatenation of N-length sequences $\{\mathbf{z}_{1,b}\}_{b=1}^{B+1}$ Define the induced distributions at both wardens, re-

spectively, by

$$\widehat{Q}_1^n(\mathbf{z}_1) \triangleq \frac{1}{(M'K')^{B+1}} \sum_{\mathbf{m}_0^B} \sum_{\mathbf{k}_0^B} W_{Z_1|X_1}^{\otimes N}\left(\mathbf{z}_{11}|\mathbf{x}_{11,(k_0,k_1)}(m_0,m_1)\right)\ldots$$

$$\ldots \times W_{Z_1|X_1}^{\otimes N}\left(\mathbf{z}_{1(B+1)}|\mathbf{x}_{1(B+1),(k_B,k_{B+1})}(m_B,m_{B+1})\right) \tag{5.193}$$

$$= \frac{1}{(M'K')^{B+1}} \sum_{\mathbf{m}_0^B} \sum_{\mathbf{k}_0^B} \left(\prod_{b=1}^{B+1} W_{Z_1|X_1}^{\otimes N}\left(\mathbf{z}_{1b}|\mathbf{x}_{1b,(k_{b-1},k_b)}(m_{b-1},m_b)\right)\right), \tag{5.194}$$

$$\widehat{Q}_2^n(\mathbf{z}_2) \triangleq \frac{1}{(M'K')^{B+1}} \sum_{\mathbf{m}_0^B} \sum_{\mathbf{k}_0^B} W_{Z_2|X_2}^{\otimes N}\left(\mathbf{z}_{21}|\mathbf{x}_{21,k_0}(m_0)\right) W_{Z_2|X_2}^{\otimes N}\left(\mathbf{z}_{22}|\mathbf{x}_{22,k_1}(m_1)\right)\ldots$$

$$\ldots \times W_{Z_2|X_2}^{\otimes N}\left(\mathbf{z}_{2(B+1)}|\mathbf{x}_{2(B+1),k_B}(m_B)\right) \tag{5.195}$$

$$= \prod_{b=1}^{B+1} \widehat{Q}_{2,b}^N(\mathbf{z}_{2b}), \tag{5.196}$$

where $\widehat{Q}_{2,b}^N(\mathbf{z}_{2b}) \triangleq \frac{1}{M'K'} \sum_{m_{b-1}} \sum_{k_{b-1}} W_{Z_2|X_2}^{\otimes N}\left(\mathbf{z}_{2b}|\mathbf{x}_{2b,k_{b-1}}(m_{b-1})\right)$.

First, we analyze the KL divergence between the induced distribution $\widehat{Q}_1^n$ at the first warden and the corresponding covert process $Q_{\alpha_n}^{\otimes n}$. For the message-key pair $\left(\mathbf{m}_0^B, \mathbf{k}_0^B\right) \in [\![1, M']\!]^{B+1} \times [\![1, K']\!]^{B+1}$, we represent the expectation taken over all random codewords $\left\{\left\{\mathbf{X}_{1b,(s_{b-1},s_b)}(u_{b-1},u_b)\right\}_{b\in[\![1,B+1]\!]}\right\}_{\left(\mathbf{u}_0^B,\mathbf{s}_0^B\right)\in[\![1,M']\!]^{B+1}\times[\![1,K']\!]^{B+1}\setminus\left(\mathbf{m}_0^B,\mathbf{k}_0^B\right)}$ by $\mathbb{E}_{\sim\left(m_0^B,k_0^B\right)}$. The KL divergence between $\widehat{Q}_1^n$ and $Q_{\alpha_n}^{\otimes n}$ averaged over all random code-

books $\mathcal{C}$ is

$$\begin{aligned}
&\mathbb{E}_{\mathcal{C}}\left(\mathbb{D}\Big(\widehat{Q}_1^n \| Q_{\alpha_n}^{\otimes n}\Big)\right) \\
&\quad= \mathbb{E}_{\mathcal{C}}\left(\sum_{\mathbf{z}_1} \widehat{Q}_1^n\left(\mathbf{z}_1\right) \log \frac{\widehat{Q}_1^n\left(\mathbf{z}_n\right)}{Q_{\alpha_n}^{\otimes n}\left(\mathbf{z}_1\right)}\right) \qquad (5.197) \\
&\quad\leqslant \sum_{\mathbf{z}_1} \frac{1}{\left(M'K'\right)^{B+1}} \sum_{\mathbf{m}_0^B} \sum_{\mathbf{k}_0^B} 1 \\
&\qquad\times \left(\prod_{b=1}^{B+1} \sum_{\mathbf{x}_{1b,(k_{b-1},k_b)}(m_{b-1},m_b)} W_{Z_1|X_1}^{\otimes N}\left(\mathbf{z}_{1b}|\mathbf{x}_{1b,(k_{b-1},k_b)}(m_{b-1},m_b)\right)\right. \\
&\qquad\qquad\left.\times \Pi_{X_1}^{\otimes N}\left(\mathbf{x}_{1b,(k_{b-1},k_b)}(m_{b-1},m_b)\right)\right) \\
&\qquad\times \log \mathbb{E}_{\sim\left(\mathbf{m}_0^B,\mathbf{k}_0^B\right)}\left(\frac{\sum_{\mathbf{u}_0^B}\sum_{\mathbf{s}_0^B}\left(\prod_{b=1}^{B+1} W_{Z_1|X_1}^{\otimes N}\left(\mathbf{z}_{1b}|\mathbf{X}_{1b,(s_{b-1},s_b)}(u_{b-1},u_b)\right)\right)}{\left(M'K'\right)^{B+1} Q_{\alpha_n}^{\otimes n}\left(\mathbf{z}_1\right)}\right). \qquad (5.198)
\end{aligned}$$

Define $\mu_1 \triangleq \min_{z_1 \in \mathcal{Z}_1} Q_0(z_1)$ and a set $\mathcal{S}_{b'} \subset [\![0, B]\!]$ such that $|\mathcal{S}_{b'}| = b'$, where $b' \in [\![1, B]\!]$. For each set $\mathcal{S}_{b'}$, we define another set $\mathcal{T}_{b'} \triangleq \{i+1 : i \in \mathcal{S}_{b'}\}$. Now, we

analyze just the log term in (5.198),

$$\log \mathbb{E}_{\sim\left(\mathbf{m}_0^B,\mathbf{k}_0^B\right)}\left(\frac{\sum_{\mathbf{u}_0^B}\sum_{\mathbf{s}_0^B}\left(\prod_{b=1}^{B+1} W_{Z_1|X_1}^{\otimes N}\left(\mathbf{z}_{1b}|\mathbf{X}_{1b,(s_{b-1},s_b)}(u_{b-1},u_b)\right)\right)}{\left(M'K'\right)^{B+1} Q_{\alpha_n}^{\otimes n}\left(\mathbf{z}_1\right)}\right)$$
$$\leqslant \log\left(\frac{\prod_{b=1}^{B+1} W_{Z_1|X_1}^{\otimes N}\left(\mathbf{z}_{1b}|\mathbf{x}_{1b,(k_{b-1},k_b)}(m_{b-1},m_b)\right)}{\left(M'K'\right)^{B+1} Q_{\alpha_n}^{\otimes n}\left(\mathbf{z}_1\right)}+1\right.$$
$$\left.+\sum_{b'=1}^{B}\frac{1}{\left(M'K'\right)^{B+1-b'}}\sum_{\mathcal{S}_{b'}\subset[\![0,B]\!]}\prod_{\substack{b=1\\ b\notin\mathcal{S}_{b'}\cup\mathcal{T}_{b'}}}^{B+1}\frac{W_{Z_1|X_1}^{\otimes N}\left(\mathbf{z}_{1b}|\mathbf{x}_{1b,(k_{b-1},k_b)}(m_{b-1},m_b)\right)}{Q_{\alpha_n}^{\otimes N}\left(\mathbf{z}_{1b}\right)}\right) \tag{5.199}$$

$$\leqslant \log\left(\left(\frac{e^{\tau_1}}{M'K'}\right)^{B+1}+\sum_{b'=1}^{B}\binom{B+1}{b'}\frac{\left(e^{\tau_1}\right)^{B-b'}}{\left(M'K'\right)^{B+1-b'}}+1\right)$$
$$+\log\left(\frac{2^{2(B+1)}}{Q_{\alpha_n}^{\otimes n}\left(\mathbf{z}_1\right)}\right)\left(\prod_{b=1}^{B+1}\mathbb{1}\left\{\left(\mathbf{x}_{1b,(k_{b-1},k_b)}(m_{b-1},m_b),\mathbf{z}_{1b}\right)\notin\mathcal{B}_{\tau_1}^N\right\}\right) \tag{5.200}$$

$$\leqslant \left(\frac{e^{\tau_1}}{M'K'}\right)^{B+1}+\sum_{b'=1}^{B}\binom{B+1}{b'}\frac{\left(e^{\tau_1}\right)^{B-b'}}{\left(M'K'\right)^{B+1-b'}}$$
$$+n\log\left(\frac{2}{\left(1-\rho_n\alpha_n\right)\mu_1}\right)\left(\prod_{b=1}^{B+1}\mathbb{1}\left\{\left(\mathbf{x}_{1b,(k_{b-1},k_b)}(m_{b-1},m_b),\mathbf{z}_{1b}\right)\notin\mathcal{B}_{\tau_1}^N\right\}\right). \tag{5.201}$$

Combining (5.198) and (5.201), we obtain

$$\mathbb{E}_{\mathcal{C}}\left(\mathbb{D}\left(\widehat{Q}_1^N\|Q_{\alpha_n}^{\otimes N}\right)\right)\leqslant\left(\frac{e^{\tau_1}}{M'K'}\right)^{B+1}+\sum_{b'=1}^{B}\binom{B+1}{b'}\frac{\left(e^{\tau_1}\right)^{B-b'}}{\left(M'K'\right)^{B+1-b'}}$$
$$+n\log\left(\frac{2}{\left(1-\rho_n\alpha_n\right)\mu_1}\right)\left(\mathbb{P}\left(\mathcal{B}_{\tau_1}^{N\,c}\right)\right)^{B+1}. \tag{5.202}$$

For an arbitrary $\mu\in(0,1)$, let us define

$$\tau_1\triangleq(1+\mu)N\mathbb{I}(X_1;Z_1). \tag{5.203}$$

Expanding $\mathbb{I}(X_1; Z_1)$, we obtain

$$\mathbb{I}(X_1; Z_1) = \rho_n \alpha_n \mathbb{D}(Q_1 \| Q_0) + \mathcal{O}\left(\alpha_n^2\right). \tag{5.204}$$

Rewriting (5.203) using (5.204), we have

$$\tau_1 = (1+\mu) N \rho_n \alpha_n \mathbb{D}(Q_1 \| Q_0) + n\mathcal{O}\left(\alpha_n^2\right). \tag{5.205}$$

Using Bernstein's inequality, we can upper bound

$$\mathbb{P}\left(\mathcal{B}_{\tau_1}^{N\,c}\right) \leqslant \exp\left(-a_4 n \alpha_n\right), \tag{5.206}$$

for an appropriate constant $a_4 > 0$. Then, if we choose M' and K' such that, for a large N,

$$\log M' + \log K' > (1+\mu) N \rho_n \alpha_n \mathbb{D}(Q_1 \| Q_0), \tag{5.207}$$

the average KL divergence at warden 1 can be upper bounded by

$$\mathbb{E}_{\mathcal{C}}\left(\mathbb{D}\left(\widehat{Q}_1^N \| Q_{\alpha_n}^{\otimes N}\right)\right) \leqslant \exp\left(-a_5 n \alpha_n\right), \tag{5.208}$$

for an appropriate constant $a_5 > 0$.

Next, we analyze the KL divergence between the induced distribution $\widehat{Q}_2^n$ at the second warden and the covert process $\overline{Q}_{\alpha_n}^{\otimes n}$. Let us denote (m_{b-1}, k_{b-1}) by (i, j). For the message-key pair $(i, j) \in [\![1, M']\!] \times [\![1, K']\!]$, we denote the expectation over all random codewords $\{\mathbf{X}_{2b,k}(\ell)\}_{(\ell,k) \in [\![1,M']\!] \times [\![1,K']\!] \setminus (i,j)}$ by $\mathbb{E}_{\sim(i,j)}$. We bound the KL

divergence between $\widehat{Q}_2^n$ and $\overline{Q}_{\alpha_n}^{\otimes n}$ averaged over all random codebooks $\mathcal{C}$ by

$$\begin{aligned}
&\mathbb{E}_{\mathcal{C}}\left(\mathbb{D}\Big(\widehat{Q}_2^n\|\overline{Q}_{\alpha_n}^{\otimes n}\Big)\right) \\
&\quad=\sum_{b=1}^{B+1}\mathbb{E}_{\mathcal{C}_b}\left(\mathbb{D}\Big(\widehat{Q}_{2,b}^N\|\overline{Q}_{\alpha_n}^{\otimes N}\Big)\right) \qquad (5.209)\\
&\quad\leqslant\sum_{b=1}^{B+1}\sum_{\mathbf{z}_{2b}}\frac{1}{M'K'}\sum_i\sum_j\sum_{\mathbf{x}_{2b,j}(i)}W_{Z_2|X_2}^{\otimes N}\left(\mathbf{z}_{2b}|\mathbf{x}_{2b,j}(i)\right)\Pi_{X_2}^{\otimes N}\left(\mathbf{x}_{2b,j}(i)\right)\\
&\qquad\qquad\times\log\mathbb{E}_{\sim(i,j)}\left(\frac{\sum_\ell\sum_k W_{Z_2|X_2}^{\otimes N}\left(\mathbf{z}_{2b}|\mathbf{X}_{2b,k}(\ell)\right)}{M'K'\overline{Q}_{\alpha_n}^{\otimes N}(\mathbf{z}_{2b})}\right). \qquad (5.210)
\end{aligned}$$

Defining $\mu_2\triangleq\min_{z_2\in\mathcal{Z}_2}\overline{Q}_0(z_2)$, we upper bound the log term in (5.210) by

$$\begin{aligned}
&\log\mathbb{E}_{\sim(i,j)}\left(\frac{\sum_\ell\sum_k W_{Z_2|X_2}^{\otimes N}\left(\mathbf{z}_{2b}|\mathbf{X}_{2b,k}(\ell)\right)}{M'K'\overline{Q}_{\alpha_n}^{\otimes N}(\mathbf{z}_{2b})}\right)\\
&\quad=\log\left(\frac{W_{Z_2|X_2}^{\otimes N}\left(\mathbf{z}_{2b}|\mathbf{x}_{2b,j}(i)\right)}{M'K'\overline{Q}_{\alpha_n}^{\otimes N}(\mathbf{z}_{2b})}\right.\\
&\qquad\qquad\left.+\frac{\sum_{\ell\neq i}\sum_{k\neq j}\sum_{\mathbf{x}_{2b,k}(\ell)}\Pi_{X_2}^{\otimes N}\left(\mathbf{x}_{2b,k}(\ell)\right)W_{Z_2|X_2}^{\otimes N}\left(\mathbf{z}_{2b}|\mathbf{X}_{2b,k}(\ell)\right)}{M'K'\overline{Q}_{\alpha_n}^{\otimes N}(\mathbf{z}_{2b})}\right) \qquad (5.211)\\
&\quad\leqslant\log\left(\frac{e^{\tau_2}}{M'K'}+1\right)\mathbb{1}\left\{(\mathbf{x}_{2b,j}(i),\mathbf{z}_{2b})\in\mathcal{B}_{\tau_2}^N\right\}\\
&\qquad+\log\left(\frac{2}{\overline{Q}_{\alpha_n}^{\otimes N}(\mathbf{z}_{2b})}\right)\mathbb{1}\left\{(\mathbf{x}_{2b,j}(i),\mathbf{z}_{2b})\notin\mathcal{B}_{\tau_2}^N\right\} \qquad (5.212)\\
&\quad\leqslant\frac{e^{\tau_2}}{M'K'}+N\log\left(\frac{2}{(1-\gamma\alpha_n)\mu_2}\right)\mathbb{1}\left\{(\mathbf{x}_{2b,j}(i),\mathbf{z}_{2b})\notin\mathcal{B}_{\tau_2}^N\right\}. \qquad (5.213)
\end{aligned}$$

Combining (5.210) and (5.213), we obtain

$$\mathbb{E}_{\mathcal{C}}\left(\mathbb{D}\Big(\widehat{Q}_2^n\|\overline{Q}_{\alpha_n}^{\otimes n}\Big)\right)\leqslant(B+1)\frac{e^{\tau_2}}{M'K'}+n\log\left(\frac{2}{(1-\gamma\alpha_n)\mu_2}\right)\mathbb{P}\big(\mathcal{B}_{\tau_2}^{Nc}\big). \qquad (5.214)$$

For an arbitrary $\mu\in(0,1)$, define

$$\tau_2\triangleq(1+\mu)N\mathbb{I}(X_2;Z_2). \qquad (5.215)$$

Expanding the mutual information term in (5.215), we obtain

$$\mathbb{I}(X_2; Z_2) = \gamma\alpha_n \mathbb{D}\big(\overline{Q}_1 \| \overline{Q}_0\big) + \mathcal{O}\left(\alpha_n^2\right). \tag{5.216}$$

Rewriting (5.215) using (5.216), we have

$$\tau_2 = (1+\mu)\, N\gamma\alpha_n \mathbb{D}\big(\overline{Q}_1 \| \overline{Q}_0\big) + n\mathcal{O}\left(\alpha_n^2\right). \tag{5.217}$$

Using Bernstein's inequality, we can upper bound

$$\mathbb{P}\big(\mathcal{B}_{\tau_2}^{N^c}\big) \leqslant \exp\left(-a_6 n\alpha_n\right), \tag{5.218}$$

for an appropriate constant $a_6 > 0$. Then, if we choose M' and K' such that, for a large n,

$$\log M' + \log K' > (1+\mu)\, N\gamma\alpha_n \mathbb{D}\big(\overline{Q}_1 \| \overline{Q}_0\big), \tag{5.219}$$

the average KL divergence at warden 2 can be upper bounded by

$$\mathbb{E}_{\mathcal{C}}\left(\mathbb{D}\Big(\widehat{Q}_2^N \| \overline{Q}_{\alpha_n}^{\otimes N}\Big)\right) \leqslant \exp\left(-a_7 n\alpha_n\right), \tag{5.220}$$

for an appropriate constant $a_7 > 0$.

CHAPTER 6
ASYNCHRONOUS COVERT COMMUNICATION

6.1 Summary

In this chapter, we consider a scenario in which Alice asynchronously communicates with Bob over a DMC while escaping detection from an adversary who observes their communication through another DMC. Specifically, Alice transmits codewords of length n and chooses the transmission epoch T uniformly at random among N available time epochs, where $N \gg n$. This deliberate symbol level-asynchronism forces the adversary to monitor a window of size N' much larger than the codeword length n and results in an increased covert throughput compared to the scenario without asynchronism. Our result generalizes a previous work in which asynchronism was introduced at the codeword level, that is, having Alice choose a transmission window among non-overlapping windows of length n.

6.2 Introduction

Many information-theoretic models implicitly assume that all terminals exactly know when communication happens. However, if communication is intermittent, which is likely the case for covert communication, users may not be synchronized [87]. The lack of synchronization turns out to be beneficial for covertness [43, 88] as it forces the adversary to look for transmitted messages over a longer time interval, even if the actual transmission happens only in a fraction of that interval. In addition, the improvement in covert throughput comes *for free* if the legitimate receiver does not require knowledge of the actual transmission time to decode correctly.

This scenario is closely related to [43, 88], in which the effect of timing uncertainty

on covert throughput over AWGN channels is analyzed. Specifically, [43] considers a scenario in which the transmitter randomly chooses a transmission window of length n out of $T(n)$ contiguous and disjoint ones, thus forcing the adversary to monitor a window of $nT(n)$ symbols. The additional burden on the adversary leads to an improved covert throughput of $\mathcal{O}\left(\min\left\{\sqrt{n\log T(n)}, n\right\}\right)$. In this paper, we extend this result by showing that the covert throughput over a DMC scales as $\mathcal{O}\left(\sqrt{n\log\theta_n}\right)$ for a transmission window of size n, where $\log\theta_n \in o\left(n\right)$ and $\log\theta_n > 0$, provided the size of the monitoring window is $\omega\left(\frac{n\theta_n}{\log\theta_n}\right)$. For instance, one achieves a covert throughput of $\mathcal{O}\left(\sqrt{n\log n}\right)$ by embedding a transmission window of size n in a monitoring window of size $\omega\left(\frac{n^2}{\log n}\right)$ instead of $\omega\left(n^2\right)$ in [43]. The main conceptual difference between our scenario and the one analyzed in [43] is that the offset between potential transmission windows is reduced to one symbol instead of n symbols; that is, instead of choosing from $T(n)$ disjoint transmission windows, the transmitter chooses from N consecutive time epochs to initiate transmission. In other words, we show that *symbol-level* asynchronism is more beneficial than *codeword-level* asynchronism. Our technical approach is also completely different and exploits ideas developed in [27, 89] together with Bernstein's inequality. Bash *et al.* also extended their result to symbol-level asynchronism later in [88]. The result in this chapter is based on the results in [90].

6.3 Asynchronous Covert Communication

Before we detail the channel model, we briefly introduce the auxiliary notation used exclusively in this chapter. Sequences of length $N' \triangleq N+n-1$ are written in boldface and sequences of length n are written in boldface with a line over it. For instance, $\mathbf{y}$ denotes a sequence of length N' while $\overline{\mathbf{y}}$ denotes a sequence of length n. Also, the n-length sequence $(y_t, y_{t+1}, y_{t+2}, \ldots, y_{t+n-1})$ is denoted by $\overline{\mathbf{y}}_t^{t+n-1}$. Note that N denotes the number of time epochs that Alice can choose to start her transmission

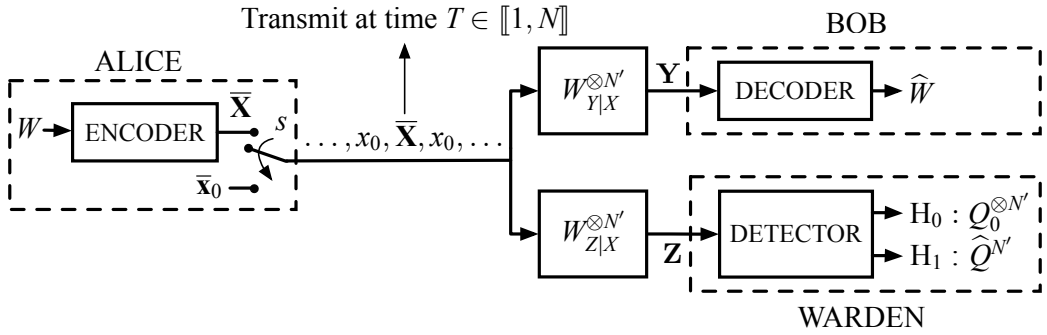

Figure 6.1: Model of asynchronous covert communication. Alice encodes message W to codeword $\overline{\mathbf{X}}$ and transmits at time T if the switch $s = 1$. Bob forms an estimate $\widehat{W}$ of W from $\mathbf{Y}$. The warden performs a hypothesis test upon observing $\mathbf{Z}$ to detect if the users communicate (H_1) or not (H_0).

in, whereas n denotes the length of the covert transmission sequence.

In this chapter, we consider the asynchronous model of covert communication illustrated in Fig.6.1. Let x_0 be the innocent symbol corresponding to the channel input when no communication takes place and $\mathbf{x}_0$ be the corresponding N' length sequence. We assume the existence of an information symbol $x_1 \in \mathcal{X}$ such that $x_1 \neq x_0$, to encode the input message. Alice encodes a message $W = i$, uniformly distributed in $[\![1, M]\!]$, into a codeword $\overline{\mathbf{X}}_i$. We denote the symbols of $\overline{\mathbf{X}}_i$ by $\overline{X}_{i,j}$, $j \in [\![1, n]\!]$.

Alice determines whether to transmit or not at the beginning of every block and fixes the state of a switch $s \in \{0, 1\}$ accordingly without any prior distribution. Alice holds the state of this switch constant throughout transmission of that block and does not disclose the state of the switch to Bob or the warden. If $s = 1$, the codeword $\overline{\mathbf{X}}_i$ is embedded in a longer sequence of x_0's by randomly choosing its start time T, i.e., $\mathbf{X} = \left(x_0, \ldots, x_0, \overline{\mathbf{X}}_i, x_0, \ldots, x_0\right)$, as shown in Fig.6.2. This sequence $\mathbf{X}$ is sent over a DMC $\left(\mathcal{X}, W_{Y|X}, \mathcal{Y}\right)$ to Bob, the legitimate receiver. We assume that Alice chooses T uniformly at random, i.e., $T \sim U(1, N)$. The warden observes the sequence $\mathbf{X}$ through another DMC $\left(\mathcal{X}, W_{Z|X}, \mathcal{Z}\right)$. Else if $s = 0$, Alice transmits the innocent sequence $\mathbf{X} = \mathbf{x}_0$. We assume that all terminals possess complete knowledge of the

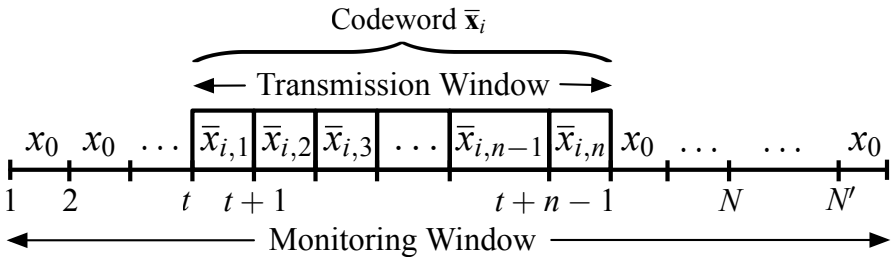

Figure 6.2: Temporal representation of the channel input. Codeword $\overline{\mathbf{x}}_i$ is transmitted starting at time t. Note that t can take any value from 1 to N.

coding scheme used. To be concise, for $k \in \{0, 1\}$, we define

$$P_k(y) \triangleq W_{Y|X}(y|x_k), \tag{6.1}$$

$$Q_k(z) \triangleq W_{Z|X}(z|x_k). \tag{6.2}$$

We assume that $Q_1 \ll Q_0$ and $Q_1 \neq Q_0$. Without this assumption, covert communication is either impossible or straightforward to achieve, which follows from reasons similar to those discussed in Chapter 3.

Bob estimates the switch state $\widehat{s}$ and only attempts to decode the transmitted message if $\widehat{s} = 1$. Reliability is measured by the metric

$$P_e \triangleq \sum_{s\in\{0,1\}} \mathbb{P}\Big(\widehat{S} \neq s\Big) + \mathbb{P}\Big(\widehat{W} \neq W | \widehat{S} = 1, s = 1\Big). \tag{6.3}$$

With a slight abuse of terminology, we call P_e the average probability of error. Define the output distributions at Bob and the warden, respectively, when communication starts at time t by

$$\widehat{P}^{N'}_{Y,t}(\mathbf{y}) \triangleq \left(\prod_{k=1}^{t-1} P_0(y_k)\right)\left(\frac{1}{M}\sum_{i=1}^{M} W^{\otimes n}_{Y|X}(\overline{\mathbf{y}}_t^{t+n-1}|\overline{\mathbf{x}}_i)\right)\left(\prod_{k=t+n}^{N'} P_0(y_k)\right), \tag{6.4}$$

$$\widehat{Q}^{N'}_{Z,t}(\mathbf{z}) \triangleq \left(\prod_{k=1}^{t-1} Q_0(z_k)\right)\left(\frac{1}{M}\sum_{i=1}^{M} W^{\otimes n}_{Z|X}(\overline{\mathbf{z}}_t^{t+n-1}|\overline{\mathbf{x}}_i)\right)\left(\prod_{k=t+n}^{N'} Q_0(z_k)\right). \tag{6.5}$$

Subsequently, we define the output distributions induced at Bob and the warden,

respectively, by

$$\widehat{P}_Y^{N'}(\mathbf{y}) \triangleq \mathbb{E}_T\left(\widehat{P}_{Y,T}^{N'}(\mathbf{y})\right), \tag{6.6}$$

$$\widehat{Q}_Z^{N'}(\mathbf{z}) \triangleq \mathbb{E}_T\left(\widehat{Q}_{Z,T}^{N'}(\mathbf{z})\right). \tag{6.7}$$

We measure covertness in terms of the KL divergence $\mathbb{D}\Big(\widehat{Q}_Z^{N'}\|Q_0^{\otimes N'}\Big)$. Ensuring that this KL divergence is negligible translates to the warden's hypothesis tests on the observation $\mathbf{Z}$ being futile. Our ultimate aim is to establish the scalings of $\log M$ and N' with n for which there exist covert communication schemes such that

$$\lim_{n\to\infty} P_e = 0, \tag{6.8}$$

$$\lim_{n\to\infty} \mathbb{D}\Big(\widehat{Q}_Z^{N'}\|Q_0^{\otimes N'}\Big) = 0. \tag{6.9}$$

Remark 4. *Since KL divergence is convex, we have*

$$\mathbb{D}\Big(\widehat{Q}_Z^{N'}\|Q_0^{\otimes N'}\Big) \leqslant \mathbb{E}_T\left(\mathbb{D}\Big(\widehat{Q}_Z^{n}\|Q_0^{\otimes n}\Big)\right). \tag{6.10}$$

However, the analysis of $\mathbb{D}\Big(\widehat{Q}_Z^{n}\|Q_0^{\otimes n}\Big)$ *according to [89] gives a rather loose upper bound and does not reveal the advantages of introducing asynchronism at the symbol level. To characterize the advantage precisely, it is vital to analyze the KL divergence* $\mathbb{D}\Big(\widehat{Q}_Z^{N'}\|Q_0^{\otimes N'}\Big)$ *more carefully.*

6.4 Covert Communication Process

As we have grown accustomed to, by now, in this chapter, we define a covert process that the induced distribution will attempt to simulate. We make certain modifications to suit our techniques to the asynchrounous setting. For $n \in \mathbb{N}^*$, let $\alpha_n \in (0,1)$.

Define the input distribution Π_X on $\{x_0, x_1\}$ by

$$\Pi_X(x_1) = 1 - \Pi_X(x_0) \triangleq \alpha_n. \tag{6.11}$$

We define the corresponding output distributions at Bob and the warden by

$$P_{\alpha_n}(y) \triangleq (1-\alpha_n)\, P_0(y) + \alpha_n P_1(y), \tag{6.12}$$

$$Q_{\alpha_n}(z) \triangleq (1-\alpha_n)\, Q_0(z) + \alpha_n Q_1(z). \tag{6.13}$$

Defining

$$P^{N'}_{\alpha_n,t}(\mathbf{y}) = \prod_{k=1}^{t-1} P_0(y_k) \prod_{k=t}^{t+n-1} P_{\alpha_n}(y_k) \prod_{k=t+n}^{N+n-1} P_0(y_k), \tag{6.14}$$

$$Q^{N'}_{\alpha_n,t}(\mathbf{z}) = \prod_{k=1}^{t-1} Q_0(z_k) \prod_{k=t}^{t+n-1} Q_{\alpha_n}(z_k) \prod_{k=t+n}^{N+n-1} Q_0(z_k), \tag{6.15}$$

we define the distributions

$$P^{N'}_{\alpha_n}(\mathbf{y}) \triangleq \mathbb{E}_T \left(P^{N'}_{\alpha_n,T}(\mathbf{y}) \right), \tag{6.16}$$

$$Q^{N'}_{\alpha_n}(\mathbf{z}) \triangleq \mathbb{E}_T \left(Q^{N'}_{\alpha_n,T}(\mathbf{z}) \right). \tag{6.17}$$

The crux of our approach is based on Lemma 14 below, which shows that the covert process $Q^{N'}_{\alpha_n}$ is nearly indistinguishable from the innocent distribution $Q_0^{\otimes N'}$ for appropriate choices of α_n and N.

Lemma 14. *Define the chi-square distance*

$$\chi \triangleq \sum_z \frac{(Q_1(z) - Q_0(z))^2}{Q_0(z)}. \tag{6.18}$$

We also define $\alpha_n \triangleq \sqrt{\frac{\log \theta_n}{n\chi}}$ *and* $N \triangleq \frac{n\theta_n}{\omega_n \log \theta_n}$, *such that* $\log \theta_n \in o(n)$, $\log \theta_n > 0$,

and $\lim_{n\to\infty}\omega_n = 0$. *Then,*

$$\lim_{n\to\infty} \mathbb{D}\Big(Q_{\alpha_n}^{N'} \| Q_0^{\otimes N'}\Big) = 0. \tag{6.19}$$

The proof of Lemma 14 is given in Appendix 6.A. Since $Q_{\alpha_n}^{N'}$ is nearly indistinguishable from $Q_0^{\otimes N'}$ for a large n and our choice of α_n and N, we only need to design a scheme that closely approximates the covert stochastic process $Q_{\alpha_n}^{N'}$ to communicate covertly with Bob.

6.5 Main Result

Our main result is the existence of asynchronous covert communication schemes that do not require a key to communicate reliably with the legitimate receiver while being simultaneously covert from an asynchronous warden.

Theorem 6. *Consider a discrete memoryless point-to-point covert channel with* $Q_1 \ll Q_0$ *and* $Q_1 \neq Q_0$. *Let* $\alpha_n \triangleq \sqrt{\frac{\log\theta_n}{n\chi}}$ *such that* $\log\theta_n \in o(n)$ *and* $\log\theta_n > 0$. *If* $\mathbb{D}(P_1\|P_0) > \mathbb{D}(Q_1\|Q_0)$, *then for any* M *that satisfies both of the following conditions, for an arbitrary* $\xi \in (0,1)$,

$$\log M \leqslant (1-\xi)n\left(\alpha_n \mathbb{D}(P_1\|P_0) + \mathcal{O}\left(\alpha_n^2\right)\right), \tag{6.20}$$

$$\log M \geqslant (1+\xi)n\left(\alpha_n \mathbb{D}(Q_1\|Q_0) + \mathcal{O}\left(\alpha_n^2\right)\right), \tag{6.21}$$

there exist $\xi_1, \xi_2 > 0$ *depending on* $\xi, W_{Y|X}, W_{Z|X}$, *and an asynchronous covert communication scheme such that for a large* n, *we have*

$$P_e \leqslant \exp\left(-\xi_1\sqrt{n\log\theta_n}\right), \tag{6.22}$$

$$\left|\mathbb{D}\Big(\widehat{Q}_Z^{N'} \| Q_0^{\otimes N'}\Big) - \mathbb{D}\Big(Q_{\alpha_n}^{N'} \| Q_0^{\otimes N'}\Big)\right| \leqslant \exp\left(-\xi_2\sqrt{n\log\theta_n}\right). \tag{6.23}$$

Proof. We rely on random coding arguments, Bernstein's inequality, and channel resolvability techniques developed in [27] and previous chapters to prove Theorem 6.

Random Codebook Generation We generate M codewords $\overline{\mathbf{x}}_i \in \{x_0, x_1\}^n$ with $i \in [\![1, M]\!]$ independently according to the distribution $\Pi_X^{\otimes n}$ defined in Section 6.4. Define the set

$$\mathcal{A}_\gamma^n \triangleq \left\{ (\overline{\mathbf{x}}, \overline{\mathbf{y}}) \in \mathcal{X}^n \times \mathcal{Y}^n : \log \frac{W_{Y|X}^{\otimes n}(\overline{\mathbf{y}}|\overline{\mathbf{x}})}{P_{\alpha_n}^{\otimes n}(\overline{\mathbf{y}})} \geqslant \gamma \right\}, \tag{6.24}$$

where $\gamma > 0$ will be defined later. The encoder at Alice maps the message $W = i$ to the codeword $\overline{\mathbf{x}}_i$ of length n, and randomly chooses a time epoch $t \in [\![1, N]\!]$ to transmit the sequence. If no message is communicated by Alice, i corresponds to a null message ϕ. Alice transmits the innocent symbol x_0 in all other channel uses.

The objective for Bob is to decode the transmitted message from the longer sequence $\mathbf{y}$ of length N' despite not knowing the time of transmission. Note that we do not require the receiver to find the correct transmission time t. The decoder at Bob operates as follows.

- Fix a n-length decoding window starting at $u = 1$.
- If there exists a unique $i \in [\![1, M]\!]$ such that $\left(\overline{\mathbf{x}}_i, \overline{\mathbf{y}}_u^{u+n-1}\right) \in \mathcal{A}_\gamma^n$, output $\widehat{W} = i$, and stop decoding. Else, increment u and iterate; that is, the decoding window slides across the monitoring window as illustrated in Figure 6.1;
- else if there is no $i \in [\![1, M]\!]$ and a choice of u such that $\left(\overline{\mathbf{x}}_i, \overline{\mathbf{y}}_u^{u+n-1}\right) \in \mathcal{A}_\gamma^n$, output $\widehat{W} = \phi$;
- else, declare a decoding error.

Channel Reliability Analysis The average decoding error probability satisfies the following lemma.

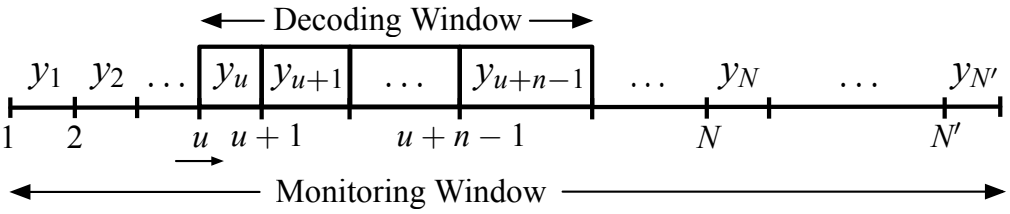

Figure 6.1: Temporal representation of the channel output.

Lemma 15. *Define* $\Lambda \triangleq \sum_y P_1(y) \log^2 \left(\frac{P_1(y)}{P_0(y)}\right)$. *For an arbitrary* $\nu \in (0,1)$, *and a large* n, *there exists* $K > 0$, *such that the probability of decoding error averaged over all random codebooks satisfies*

$$\mathbb{E}_{\mathcal{C}}\left(P_e\right) \leqslant 2NMe^{-\gamma} + \exp\left(\frac{-\frac{1}{2}\nu^2 n\left(\alpha_n \mathbb{D}^2(P_1||P_0) + \mathcal{O}\left(\alpha_n^2\right)\right)}{\Lambda + \mathcal{O}\left(\alpha_n\right) + \frac{K}{3}\nu\mathbb{D}(P_1\|P_0)}\right), \tag{6.25}$$

with

$$\gamma = (1-\nu)n\left(\alpha_n \mathbb{D}(P_1\|P_0) + \mathcal{O}\left(\alpha_n^2\right)\right) \tag{6.26}$$

The proof of Lemma 15 follows the reliability analysis techniques used in previous chapters. Hence, for the choice of α_n and θ_n in Theorem 6 and for an arbitrary $\delta \in (0,1)$, if

$$\log M = (1-\delta)(1-\nu)n\left(\alpha_n \mathbb{D}(P_1\|P_0) + \mathcal{O}\left(\alpha_n^2\right)\right), \tag{6.27}$$

there exists a constant $\xi_1' > 0$, such that for a large n,

$$\mathbb{E}\left(P_e\right) \leqslant \exp\left(-\xi_1' \sqrt{n \log \theta_n}\right). \tag{6.28}$$

Channel Resolvability Analysis Based on the discussion of Section 6.4, it is sufficient to show that the induced distribution $\widehat{Q}_Z^{N'}$ is close to $Q_{\alpha_n}^{N'}$ in KL divergence.

Lemma 16. *Define*

$$\Lambda' \triangleq \sum_z Q_1(z) \log^2 \left(\frac{Q_1(z)}{Q_0(z)} \right). \tag{6.29}$$

For an arbitrary $\nu \in (0,1)$, $\mu_0 \triangleq \min_z Q_0(z)$, *and* n *large enough, there exists* $K' > 0$ *such that the KL divergence between* $\widehat{Q}_Z^{N'}$ *and* $Q_{\alpha_n}^{N'}$ *averaged over all random codebooks satisfies*

$$\mathbb{E}\left(\mathbb{D}\left(\widehat{Q}_Z^{N'} \| Q_{\alpha_n}^{N'} \right) \right) \leqslant \frac{e^\tau}{M} + n \log \left(\frac{2}{(1-\alpha_n)\,\mu_0} \right) \times \exp \left(\frac{-\frac{1}{2}\nu^2 n \left(\alpha_n \mathbb{D}^2(Q_1||Q_0) + \mathcal{O}\left(\alpha_n^2\right) \right)}{\Lambda' + \mathcal{O}\left(\alpha_n\right) + \frac{K'}{3}\nu \mathbb{D}(Q_1 \| Q_0)} \right), \tag{6.30}$$

with $\tau = (1+\nu)\, n \left(\alpha_n \mathbb{D}(Q_1 \| Q_0) + \mathcal{O}\left(\alpha_n^2\right) \right)$.

The proof of Lemma 16 follows the channel resolvability techniques used in previous chapters. Hence, for the choice of α_n and θ_n in Theorem 6 and for any $\delta \in (0,1)$, if

$$\log M = (1+\delta)\,(1+\nu)\, n \left(\alpha_n \mathbb{D}(Q_1 \| Q_0) + \mathcal{O}\left(\alpha_n^2\right) \right), \tag{6.31}$$

there exists a constant $\xi_2' > 0$, such that for n large enough

$$\mathbb{E}\left(\mathbb{D}\left(\widehat{Q}_Z^{N'} \| Q_{\alpha_n}^{N'} \right) \right) \leqslant \exp\left(-\xi_2' \sqrt{n \log \theta_n} \right). \tag{6.32}$$

Identification of a code Following the same arguments as in [27] to identify a code, we show that there exists at least one asynchronous coding scheme such that

for appropriate $\xi_1, \xi_2'' > 0$ and a large n, we have

$$P_e \leqslant \exp\left(-\xi_1 \sqrt{n \log \theta_n}\right), \tag{6.33}$$

$$\mathbb{D}\left(\widehat{Q}_Z^{N'} \| Q_{\alpha_n}^{N'}\right) \leqslant \exp\left(-\xi_2'' \sqrt{n \log \theta_n}\right), \tag{6.34}$$

and that for this specific code there exists a constant $\xi_2 > 0$ such that

$$\left|\mathbb{D}\left(\widehat{Q}_Z^{N'} \| Q_0^{\otimes N'}\right) - \mathbb{D}\left(Q_{\alpha_n}^{N'} \| Q_0^{\otimes N'}\right)\right| \leqslant \exp\left(-\xi_2 \sqrt{n \log \theta_n}\right). \tag{6.35}$$

□

APPENDIX

6.A Proof of Lemma 14

Defining $\Psi(z) \triangleq \frac{Q_1(z)-Q_0(z)}{Q_0(z)}$, we write

$$\mathbb{D}\Big(Q_{\alpha_n}^{N'} \| Q_0^{\otimes N'}\Big) = \sum_{\mathbf{z}} Q_{\alpha_n}^{N'}(\mathbf{z}) \log \sum_{t=1}^{N} \frac{1}{N} \frac{Q_{\alpha_n,t}^{N'}(\mathbf{z})}{Q_0^{\otimes N'}(\mathbf{z})} \tag{6.36}$$

$$= \sum_{\mathbf{z}} Q_{\alpha_n}^{N'}(\mathbf{z}) \log \sum_{t=1}^{N} \frac{1}{N} \prod_{i=t}^{t+n-1} \frac{Q_{\alpha_n}(z_i)}{Q_0(z_i)} \tag{6.37}$$

$$= \sum_{\mathbf{z}} Q_{\alpha_n}^{N'}(\mathbf{z}) \log \sum_{t=1}^{N} \frac{1}{N} \prod_{i=t}^{t+n-1} \left(1 + \alpha_n \Psi(z_i)\right). \tag{6.38}$$

We define a set $\{\mathcal{S}_{i,1}, \mathcal{S}_{i,2}, \ldots, \mathcal{S}_{i,i}\} \subseteq [\![t, t+n-1]\!]$ of cardinality i by $\mathcal{S}_i$. We assume that the elements of $\mathcal{S}_i$ are ordered, that is, $\mathcal{S}_{i,j} < \mathcal{S}_{i,j+k}$ for $j, k > 0$. We upper bound (6.38) by

$$\mathbb{D}\Big(Q_{\alpha_n}^{N'} \| Q_0^{\otimes N'}\Big) = \frac{1}{N} \sum_{u=1}^{N} \sum_{\mathbf{z}} Q_{\alpha_n,u}^{N'}(\mathbf{z}) \log \left(1 + \frac{1}{N} \sum_{t=1}^{N} \sum_{i=1}^{n} \alpha_n^i \sum_{\mathcal{S}_i \subseteq [\![t,t+n-1]\!]} \prod_{j=1}^{i} \Psi(z_{\mathcal{S}_{i,j}})\right) \tag{6.39}$$

$$\leqslant \frac{1}{N^2} \sum_{u=1}^{N} \sum_{t=1}^{N} \sum_{i=1}^{n} \alpha_n^i \sum_{\mathcal{S}_i \subseteq [\![t,t+n-1]\!]} \sum_{\mathbf{z}} Q_{\alpha_n,u}^{N'}(\mathbf{z}) \prod_{j=1}^{i} \Psi(z_{\mathcal{S}_{i,j}}) \tag{6.40}$$

$$= \frac{1}{N^2} \sum_{u=1}^{N} \sum_{t=1}^{N} \sum_{i=1}^{n} \alpha_n^i \sum_{\mathcal{S}_i \subseteq [\![t,t+n-1]\!]} \prod_{j=1}^{i} \sum_{z_{\mathcal{S}_{i,j}}} Q_{\alpha_n,u}(z_{\mathcal{S}_{i,j}}) \Psi(z_{\mathcal{S}_{i,j}}) \tag{6.41}$$

$$\overset{(a)}{\leqslant} \frac{1}{N^2} \sum_{u=1}^{N} \sum_{t=1}^{N} \sum_{i=1}^{n} \alpha_n^{2i} \chi^i \sum_{\mathcal{S}_i \subseteq [\![t,t+n-1]\!]} \mathbb{1}\{\mathcal{S}_i \subseteq [\![u, u+n-1]\!]\} \tag{6.42}$$

$$= \frac{1}{N^2} \sum_{u=1}^{N} \sum_{t=\max(1,u-n+1)}^{\min(N,u+n-1)} \sum_{i=1}^{n} \alpha_n^{2i} \chi^i \sum_{\mathcal{S}_i \subseteq [\![t,t+n-1]\!]} \mathbb{1}\{\mathcal{S}_i \subseteq [\![u, u+n-1]\!]\} \tag{6.43}$$

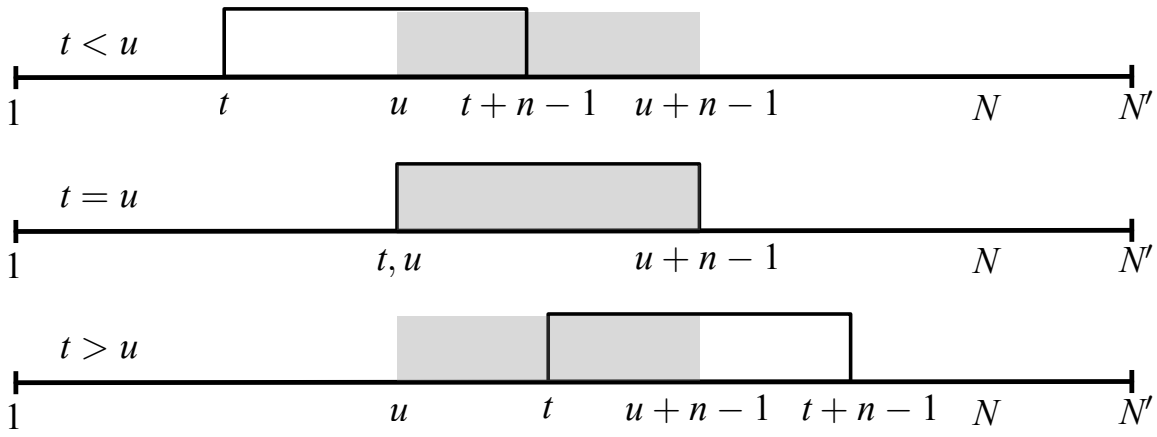

Figure 6.A.1: Windows of length n starting at t and u.

$$\begin{aligned}
&\overset{(b)}{=} \frac{1}{N^2}\Bigg(\sum_{u=2}^{N}\sum_{t=\max(1,u-n+1)}^{u-1}\sum_{i=1}^{t+n-u}\alpha_n^{2i}\chi^i\sum_{\mathcal{S}_i\subseteq[\![u,t+n-1]\!]}1 \\
&\qquad+\sum_{u=1}^{N}\sum_{i=1}^{n}\alpha_n^{2i}\chi^i\sum_{\mathcal{S}_i\subseteq[\![u,u+n-1]\!]}1 \\
&\qquad+\sum_{u=1}^{N-1}\sum_{t=u+1}^{\min(N,u+n-1)}\sum_{i=1}^{u+n-t}\alpha_n^{2i}\chi^i\sum_{\mathcal{S}_i\subseteq[\![t,u+n-1]\!]}1\Bigg) \qquad (6.44)\\
&= \frac{1}{N^2}\Bigg(\sum_{u=2}^{N}\sum_{t=\max(1,u-n+1)}^{u-1}\sum_{i=1}^{t+n-u}\alpha_n^{2i}\chi^i\binom{t+n-u}{i} \\
&\qquad+\sum_{u=1}^{N}\sum_{i=1}^{n}\alpha_n^{2i}\chi^i\binom{n}{i}+\sum_{u=1}^{N-1}\sum_{t=u+1}^{\min(N,u+n-1)}\sum_{i=1}^{u+n-t}\alpha_n^{2i}\chi^i\binom{u+n-t}{i}\Bigg), \\
&\qquad (6.45)
\end{aligned}$$

where (a) follows from the definitions of $Q_{\alpha_n,u}(z)$ and $\Psi(z)$ that ensure that

$$\prod_{j=1}^{i}\sum_{z_{\mathcal{S}_{i,j}}}Q_{\alpha_n,u}(z_{\mathcal{S}_{i,j}})\Psi(z_{\mathcal{S}_{i,j}}) = \begin{cases}\alpha_n^i\chi^i, \text{if } \mathcal{S}_i\subseteq[\![u,u+n-1]\!]\\ 0 \quad\quad, \text{else,}\end{cases} \qquad (6.46)$$

and (b) follows from splitting the sums based on whether t is smaller, equal to, or larger than u as illustrated in Figure 6.A.1. Define $\beta_n \triangleq 1+\alpha_n^2\chi$. We rewrite the

first term on the right hand side of (6.45) by splitting the sum over u as follows.

$$\begin{aligned}
&\frac{1}{N^2}\sum_{u=2}^{N}\sum_{t=\max(1,u-n+1)}^{u-1}\sum_{i=1}^{t+n-u}\alpha_n^{2i}\chi^i\binom{t+n-u}{i}\\
&\quad=\frac{1}{N^2}\sum_{u=2}^{N}\sum_{t=\max(1,u-n+1)}^{u-1}\left(\beta_n^{t+n-u}-1\right)\\
&\quad=\frac{1}{N^2}\left(\sum_{u=2}^{n-1}\sum_{t=1}^{u-1}\left(\beta_n^{t+n-u}-1\right)+\sum_{u=n}^{N}\sum_{t=u-n+1}^{u-1}\left(\beta_n^{t+n-u}-1\right)\right). \qquad (6.47)
\end{aligned}$$

On further simplification using the properties of geometric and arithmetico-geometric sequences, we obtain

$$\begin{aligned}
&\frac{1}{N^2}\sum_{u=2}^{N}\sum_{t=\max(1,u-n+1)}^{u-1}\sum_{i=1}^{t+n-u}\alpha_n^{2i}\chi^i\binom{t+n-u}{i}\\
&\quad=\frac{1}{N^2}\left(\frac{\beta_n^2+\beta_n^n\left((n-2)\left(\beta_n-1\right)-1\right)}{\left(\beta_n-1\right)^2}-\frac{(n-1)(n-2)}{2}\right)\\
&\qquad+\frac{N-n+1}{N^2}\left(\frac{\beta_n^n-\beta_n}{\beta_n-1}-\frac{n(n-1)}{2}\right). \qquad (6.48)
\end{aligned}$$

We rewrite the second term in (6.45) as

$$\frac{1}{N^2}\sum_{u=1}^{N}\sum_{i=1}^{n}\alpha_n^{2i}\chi^i\binom{n}{i}=\frac{1}{N}\left(\beta_n^n-1\right). \qquad (6.49)$$

By symmetry with the first term in (6.45), we rewrite the third term on the right hand side of (6.45) by

$$\begin{aligned}
&\frac{1}{N^2}\sum_{u=1}^{N-1}\sum_{t=u+1}^{\min(N,u+n-1)}\sum_{i=1}^{u+n-t}\alpha_n^{2i}\chi^i\binom{u+n-t}{i}\\
&\quad=\frac{1}{N^2}\sum_{t=1}^{N-n+1}\sum_{s=t+1}^{t+n-1}\sum_{i=1}^{t+n-s}\alpha_n^{2i}\chi^i\binom{t+n-s}{i}\\
&\qquad+\frac{1}{N^2}\sum_{t=N-n+2}^{N-1}\sum_{s=t+1}^{N}\sum_{i=1}^{t+n-s}\alpha_n^{2i}\chi^i\binom{t+n-s}{i} \qquad (6.50)
\end{aligned}$$

$$= \frac{1}{N^2}\left(\frac{\beta_n^2 + \beta_n^n\left((n-2)\left(\beta_n - 1\right) - 1\right)}{(\beta_n - 1)^2} - \frac{(n-1)(n-2)}{2}\right) + \frac{N-n+1}{N^2}\left(\frac{\beta_n^n - \beta_n}{\beta_n - 1} - \frac{n(n-1)}{2}\right). \tag{6.51}$$

Combining (6.48), (6.49), and (6.51), with (6.45) we upper bound $\mathbb{D}\Big(Q_{\alpha_n}^{N'} \| Q_0^{\otimes N'}\Big)$ by

$$\mathbb{D}\Big(Q_{\alpha_n}^{N'} \| Q_0^{\otimes N'}\Big) \leqslant \frac{1}{N}\left(\beta_n^n - 1\right) + \frac{2(N-n+1)}{N^2}\left(\frac{\beta_n^n - \beta_n}{\beta_n - 1}\right) + \frac{2}{N^2}\left(\frac{\beta_n^2 + \beta_n^n\left((n-2)\left(\beta_n - 1\right) - 1\right)}{(\beta_n - 1)^2}\right). \tag{6.52}$$

Now, we need to choose N carefully to ensure that $\lim_{n\to\infty} \mathbb{D}\Big(Q_{\alpha_n}^{N'} \| Q_0^{\otimes N'}\Big) = 0$. We analyze each term in (6.52) separately and ultimately choose the value of N that makes all terms in (6.52) vanish. Using the definition of β_n, we bound the first term in (6.52) by

$$\frac{1}{N}\left(\beta_n^n - 1\right) \leqslant \frac{1}{N}\exp\left(n\alpha_n^2\chi\right) = \frac{\theta_n}{N}. \tag{6.53}$$

Similarly, for the second term in (6.52), we have

$$\frac{2(N-n+1)}{N^2}\left(\frac{\beta_n^n - \beta_n}{\beta_n - 1}\right) \leqslant \frac{2(N-n+1)}{N^2}\left(\frac{\left(1+\alpha_n^2\chi\right)^n - 1 - \alpha_n^2\chi}{\alpha_n^2\chi}\right) \tag{6.54}$$

$$\leqslant \frac{2(N-n+1)}{N^2}\left(\frac{\exp\left(n\alpha_n^2\chi\right) - 1 - \alpha_n^2\chi}{\alpha_n^2\chi}\right) \tag{6.55}$$

$$= \frac{2(N-n+1)}{N^2}\left(\frac{\theta_n - 1 - \frac{\log\theta_n}{n}}{\frac{\log\theta_n}{n}}\right) \tag{6.56}$$

$$\leqslant \frac{2(N-n+1)}{N^2}\left(\frac{n\theta_n - n}{\log\theta_n}\right) \tag{6.57}$$

$$\leqslant \frac{2}{N}\left(\frac{n\theta_n}{\log\theta_n}\right). \tag{6.58}$$

Analyzing the third term in (6.52), we obtain

$$\frac{2}{N^2}\left(\frac{\beta_n^2+\beta_n^n\left((n-2)\left(\beta_n-1\right)-1\right)}{(\beta_n-1)^2}\right)\leqslant\frac{2}{N^2}\left(\frac{\beta_n^2+\beta_n^n\left((n-2)\left(\beta_n-1\right)-1\right)}{(\beta_n-1)^2}\right) \tag{6.59}$$

$$=2\left(\frac{1+\alpha_n^2\chi}{N\alpha_n^2\chi}\right)^2+\frac{\left(1+\alpha_n^2\chi\right)^n\left(n\alpha_n^2\chi-1\right)}{\left(N\alpha_n^2\chi\right)^2} \tag{6.60}$$

$$\leqslant 2\left(\frac{1}{N\alpha_n^2\chi}+\frac{1}{N}\right)^2+\frac{\exp\left(n\alpha_n^2\chi\right)\left(n\alpha_n^2\chi\right)}{\left(N\alpha_n^2\chi\right)^2} \tag{6.61}$$

$$=2\left(\frac{n}{N\log\theta_n}+\frac{1}{N}\right)^2+\frac{n^2\theta_n\log\theta_n}{N^2\log^2\theta_n} \tag{6.62}$$

$$\leqslant 2\left(\left(\frac{n}{N\log\theta_n}+\frac{1}{N}\right)^2+\frac{n^2\theta_n}{N^2\log\theta_n}\right). \tag{6.63}$$

Combining the analysis of all terms in (6.52), we conclude that for a given θ_n, we need the size of the monitoring window to be $\omega\left(\frac{n\theta_n}{\log\theta_n}\right)$ for $\mathbb{D}\left(Q_{\alpha_n}^{N'}\|Q_0^{\otimes N'}\right)$ to be negligible.

REFERENCES

[1] H. K. Melton and R. Wallace, *The official CIA manual of trickery and deception*. William Morrow New York, 2009.

[2] D. Kahn, "The history of steganography," in *International Workshop on Information Hiding*, Springer, 1996, pp. 1–5.

[3] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[4] G. J. Simmons, "The prisoners' problem and the subliminal channel," in *Advances in Cryptology*, Springer, 1984, pp. 51–67.

[5] S. Trivedi and R. Chandramouli, "Active steganalysis of sequential steganography," in *Security and Watermarking of Multimedia Contents V*, International Society for Optics and Photonics, vol. 5020, 2003, pp. 123–131.

[6] M. Basseville and I. V. Nikiforov, *Detection of abrupt changes: theory and application*. Prentice Hall Englewood Cliffs, 1993, vol. 104.

[7] U. M. Maurer, "A unified and generalized treatment of authentication theory," in *Annual Symposium on Theoretical Aspects of Computer Science*, Springer, 1996, pp. 387–398.

[8] C. Cachin, "An information-theoretic model for steganography," in *International Workshop on Information Hiding*, Springer, 1998, pp. 306–318.

[9] A. D. Ker, "Batch steganography and pooled steganalysis," in *International Workshop on Information Hiding*, Springer, 2006, pp. 265–281.

[10] ——, "A capacity result for batch steganography," *IEEE Signal Processing Letters*, vol. 14, no. 8, pp. 525–528, 2007.

[11] J. Fridrich, *Steganography in digital media: principles, algorithms, and applications*. Cambridge University Press, 2009.

[12] A. D. Ker, "The square root law requires a linear key," in *Proc. of the 11th ACM workshop on Multimedia and security*, ACM, 2009, pp. 85–92.

[13] ——, "The square root law does not require a linear key," in *Proc. of the 12th ACM workshop on Multimedia and security*, ACM, 2010, pp. 213–224.

[14] T. Filler, A. D. Ker, and J. Fridrich, "The square root law of steganographic capacity for markov covers," in *Media Forensics and Security*, International Society for Optics and Photonics, vol. 7254, 2009, p. 725 408.

[15] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," *IEEE Journal on selected areas in communications*, vol. 16, no. 4, pp. 474–481, 1998.

[16] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "A secure, robust watermark for multimedia," in *International Workshop on Information Hiding*, Springer, 1996, pp. 185–206.

[17] R. L. Peterson, R. E. Ziemer, and D. E. Borth, *Introduction to spread-spectrum communications*. Prentice hall New Jersey, 1995, vol. 995.

[18] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, "Spread spectrum communications handbook," Electronic communications, 1994.

[19] H. Urkowitz, "Energy detection of unknown deterministic signals," *Proc. of the IEEE*, vol. 55, no. 4, pp. 523–531, 1967.

[20] J. Vartiainen, J. J. Lehtomaki, and H. Saarnisaari, "Double-threshold based narrowband signal extraction," in *Proc. of IEEE 61st Vehicular Technology Conference*, vol. 2, 2005, pp. 1288–1292.

[21] Z. Deng, L. Shen, N. Bao, B. Su, J. Lin, and D. Wang, "Autocorrelation based detection of DSSS signal for cognitive radio system," in *Wireless Communications and Signal Processing (WCSP), 2011 International Conference on*, IEEE, 2011, pp. 1–5.

[22] W. A. Gardner and C. M. Spooner, "Signal interception: Performance advantages of cyclic-feature detectors," *IEEE Transactions on Communications*, vol. 40, no. 1, pp. 149–159, 1992.

[23] J. Yan and J. Hongbing, "A cyclic-cumulant based method for DSSS signal detection and parameter estimation," in *Microwave, Antenna, Propagation and EMC Technologies for Wireless Communications, 2005. MAPE 2005. IEEE International Symposium on*, IEEE, vol. 2, 2005, pp. 966–969.

[24] J. Chuang and R. M. Narayanan, "Performance of non-polarized noise modulated communications system in the presence of interference," *Wireless Personal Communications*, vol. 65, no. 4, pp. 773–796, 2012.

[25] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1921–1930, 2013.

[26] T. M. Cover and J. A. Thomas, "Elements of information theory 2nd edition," 2006.

[27] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2334–2354, 2016.

[28] E. Lehmann and J. P. Romano, *Testing Statistical Hypotheses, 3ed*, 1. 2014, pp. 1–5, ISBN: 9780874216561.

[29] M. Tahmasbi and M. R. Bloch, "First and second order asymptotics in covert communication," *IEEE Transactions on Information Theory*, pp. 1–1, 2018.

[30] A. O. Hero, "Secure space-time communication," *IEEE Transactions on Information Theory*, vol. 49, no. 12, pp. 3235–3249, 2003.

[31] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Communications Magazine*, vol. 53, no. 12, pp. 26–31, 2015.

[32] P. H. Che, M. Bakshi, and S. Jaggi, "Reliable deniable communication: Hiding messages in noise," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Istanbul, Turkey, 2013, pp. 2945–2949.

[33] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3493–3503, 2016.

[34] M. Tahmasbi, M. R. Bloch, and V. Y. Tan, "Error exponent for covert communications over discrete memoryless channels," in *Proc. of IEEE Information Theory Workshop (ITW)*, IEEE, 2017, pp. 304–308.

[35] P. H. Che, M. Bakshi, C. Chan, and S. Jaggi, "Reliable, deniable and hidable communication," in *Proc. of IEEE Information Theory and Applications Workshop (ITA)*, San Diego, CA, 2014, pp. 1–10.

[36] S. Kadhe, S. Jaggi, M. Bakshi, and A. Sprintson, "Reliable, deniable, and hidable communication over multipath networks," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Honolulu, HI, 2014, pp. 611–615.

[37] P. H. Che, M. Bakshi, C. Chan, and S. Jaggi, "Reliable deniable communication with channel uncertainty," in *Proc. of IEEE Information Theory Workshop (ITW)*, Hobart, Australia, 2014, pp. 30–34.

[38] S. Lee and R. J. Baxley, "Achieving positive rate with undetectable communication over AWGN and rayleigh channels," in *Proc. of IEEE International Conference on Communications (ICC)*, Sydney, Australia, 2014, pp. 780–785.

[39] S. Lee, R. J. Baxley, M. A. Weitnauer, and B. Walkenhorst, "Achieving undetectable communication," *IEEE Journal of Selected Topics in Signal Processing*, vol. 9, no. 7, pp. 1195–1205, 2015.

[40] R. Tandra and A. Sahai, "SNR walls for signal detection," *IEEE Journal of Selected Topics in Signal Processing*, vol. 2, no. 1, pp. 4–17, 2008.

[41] S. Lee, R. J. Baxley, J. B. McMahon, and R. S. Frazier, "Achieving positive rate with undetectable communication over MIMO rayleigh channels," in *Proc. of IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, A Coruña, Spain, 2014, pp. 257–260.

[42] S.-H. Lee, L. Wang, A. Khisti, and G. W. Wornell, "Covert communication with channel-state information at the transmitter," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 9, pp. 2310–2319, 2018.

[43] B. A. Bash, D. Goeckel, and D. Towsley, "LPD communication when the warden does not know when," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Honolulu, HI, 2014, pp. 606–610.

[44] D. Goeckel, B. Bash, S. Guha, and D. Towsley, "Covert communications when the warden does not know the background noise power," *IEEE Communications Letters*, vol. 20, no. 2, pp. 236–239, 2016.

[45] V. Anantharam and S. Verdu, "Bits through queues," *IEEE Transactions on Information Theory*, vol. 42, no. 1, pp. 4–18, 1996.

[46] R. Soltani, D. Goeckel, D. Towsley, and A. Houmansadr, "Covert communications on poisson packet channels," in *Proc. of IEEE 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2015, pp. 1046–1052.

[47] P. Mukherjee and S. Ulukus, "Covert bits through queues," in *Proc. of IEEE Conference on Communications and Network Security (CNS)*, Philadelphia, PA, 2016, pp. 626–630.

[48] R. Soltani, D. Goeckel, D. Towsley, and A. Houmansadr, "Fundamental limits of covert bit insertion in packets," in *Proc. of IEEE 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2018, pp. 1065–1072.

[49] R. Soltani, D. Goeckel, D. Towsley, B. A. Bash, and S. Guha, "Covert wireless communication with artificial noise generation," *IEEE Transactions on Wireless Communications*, vol. 17, no. 11, pp. 7252–7267, 2018.

[50] A. Sheikholeslami, M. Ghaderi, D. Towsley, B. A. Bash, S. Guha, and D. Goeckel, "Multi-hop routing in covert wireless networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 6, pp. 3656–3669, 2018.

[51] Q. Zhang, M. Bakshi, and S. Jaggi, "Computationally efficient deniable communication," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Barcelona, Spain, 2016, pp. 2234–2238.

[52] M. R. Bloch and S. Guha, "Optimal covert communications using pulse-position modulation," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Aachen, Germany, 2017, pp. 2825–2829.

[53] G. Frèche, M. R. Bloch, and M. Barret, "Polar codes for covert communications over asynchronous discrete memoryless channels," *Entropy*, vol. 20, no. 1, p. 3, 2017.

[54] I. A. Kadampot, M. Tahmasbi, and M. R. Bloch, "Multilevel-coded pulse-position modulation for covert communications over binary-input discrete memoryless channels," *CoRR*, vol. abs/1811.09695, 2018. arXiv: `1811.09695`.

[55] M. Tahmasbi and M. R. Bloch, "Covert secret key generation," in *Proc. of IEEE Conference on Communications and Network Security (CNS)*, Las Vegas, NV, 2017, pp. 540–544.

[56] M. Tahmasbi and M. Bloch, "Covert secret key generation with an active warden," *CoRR*, vol. abs/1901.02044, 2019. arXiv: `1901.02044`.

[57] B. A. Bash, S. Guha, D. Goeckel, and D. Towsley, "Quantum noise limited optical communication with low probability of detection," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Istanbul, Turkey, 2013, pp. 1715–1719.

[58] B. A. Bash, A. H. Gheorghe, M. Patel, J. L. Habif, D. Goeckel, D. Towsley, and S. Guha, "Quantum-secure covert communication on bosonic channels," *Nature communications*, vol. 6, p. 8626, 2015.

[59] A. Sheikholeslami, B. A. Bash, D. Towsley, D. Goeckel, and S. Guha, "Covert communication over classical-quantum channels," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Barcelona, Spain, 2016, pp. 2064–2068.

[60] L. Wang, "Optimal throughput for covert communication over a classical-quantum channel," in *Proc. of IEEE Information Theory Workshop (ITW)*, Cambridge, UK, 2016, pp. 364–368.

[61] J. Hou, G. Kramer, and M. Bloch, "Effective secrecy: Reliability, confusion, and stealth," in *Information Theoretic Security and Privacy of Information Systems*, R. F. Schaefer, H. Boche, A. Khisti, and H. V. Poor, Eds. Cambridge University Press, 2017, pp. 3–20.

[62] J. Hou and G. Kramer, "Effective secrecy: Reliability, confusion and stealth," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Honolulu, HI, 2014, pp. 601–605.

[63] T. S. Han and S. Verdú, "Approximation theory of output statistics," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 752–772, 1993.

[64] Y. Steinberg, "Resolvability theory for the multiple-access channel," *IEEE Transactions on Information Theory*, vol. 44, no. 2, pp. 472–487, 1998.

[65] M. H. Yassaee and M. R. Aref, "Multiple access wiretap channels with strong secrecy," in *Proc. of IEEE Information Theory Workshop*, Dublin, Ireland, 2010.

[66] M. Frey, I. Bjelaković, and S. Stańczak, "MAC resolvability: First and second order results," in *Proc. of IEEE Conference on Communications and Network Security (CNS)*, 2017, pp. 560–564.

[67] S. Verdu, "On channel capacity per unit cost," *IEEE Transactions on Information Theory*, vol. 36, no. 5, pp. 1019–1030, 1990.

[68] K. S. K. Arumugam and M. R. Bloch, "Keyless covert communication over multiple-access channels," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Barcelona, Spain, 2016, pp. 2229–2233.

[69] ——, "Covert communication over a K-user multiple access channel," *arXiv preprint arXiv:1803.06007*, 2018.

[70] E. L. Lehmann and J. P. Romano, *Testing statistical hypotheses*. Springer Science & Business Media, 2006.

[71] P. Cuff, "Distributed channel synthesis," *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7071–7096, 2013.

[72] M. Hayashi, "General nonasymptotic and asymptotic formulas in channel resolvability and identification capacity and their application to the wiretap chan-

nel," *IEEE Transactions on Information Theory*, vol. 52, no. 4, pp. 1562–1575, 2006.

[73] H. Endo, M. Sasaki, *et al.*, "Reliability and secrecy functions of the wiretap channel under cost constraint," *IEEE Transactions on Information Theory*, vol. 60, no. 11, pp. 6819–6843, 2014.

[74] M. B. Parizi, E. Telatar, and N. Merhav, "Exact random coding secrecy exponents for the wiretap channel," *IEEE Transactions on Information Theory*, vol. 63, no. 1, pp. 509–531, 2017.

[75] N. Helhal, M. Bloch, and A. Nosratinia, "Multiple-access channel resolvability with cribbing," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Vail, CO, 2018, pp. 2052–2056.

[76] N. Helal, M. Bloch, and A. Nosratinia, "Cooperative resolvability and secrecy in the cribbing multiple-access channel," *CoRR*, vol. abs/1811.11649, 2018. arXiv: 1811.11649.

[77] A. Dutta, D. Saha, D. Grunwald, and D. Sicker, "Secret agent radio: Covert communication through dirty constellations," in *International Workshop on Information Hiding*, Springer, Berkeley, CA, 2012, pp. 160–175.

[78] V. Y. F. Tan and S. Lee, "Time-division transmission is optimal for covert communication over broadcast channels," *arXiv preprint arXiv:1710.09754*, 2017.

[79] K. S. K. Arumugam and M. R. Bloch, "Covert communication over broadcast channels," in *Proc. of IEEE Information Theory Workshop (ITW)*, Kaohsiung, Taiwan, 2017, pp. 299–303.

[80] K. S. K. Arumugam and M. R. Bloch, "Embedding covert information in broadcast communications," *arXiv preprint arXiv:1808.09556*, 2018.

[81] R. G. Gallager, *Information theory and reliable communication*. Springer, 1968, vol. 2.

[82] I. Csiszar and J. Körner, *Information theory: coding theorems for discrete memoryless systems*. Cambridge University Press, 2011.

[83] J. Hu, S. Yan, X. Zhou, F. Shu, J. Li, and J. Wang, "Covert communication achieved by a greedy relay in wireless networks," *IEEE Transactions on Wireless Communications*, vol. 17, no. 7, pp. 4766–4779, 2018.

[84] K. S. K. Arumugam, M. R. Bloch, and L. Wang, "Covert communication over a physically degraded relay channel with non-colluding wardens," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, Vail, CO, 2018.

[85] A. El Gamal and Y. H. Kim, *Network information theory*. Cambridge University Press, 2011.

[86] G. Kramer, "Topics in multi-user information theory," *Foundations and Trends in Communications and Information Theory*, vol. 4, no. 4–5, pp. 265–444, 2008.

[87] A. Tchamkerten, V. Chandar, and G. W. Wornell, "Communication under strong asynchronism," *IEEE Transactions on Information Theory*, vol. 55, no. 10, pp. 4508–4528, 2009.

[88] B. A. Bash, D. Goeckel, and D. Towsley, "Covert communication gains from adversary's ignorance of transmission time," *IEEE Transactions on Wireless Communications*, vol. 15, no. 12, pp. 8394–8405, 2016.

[89] M. Bloch, "A channel resolvability perspective on stealth communications," in *Proc. of IEEE International Symposium on Information Theory (ISIT)*, 2015, pp. 2535–2539.

[90] K. S. K. Arumugam and M. R. Bloch, "Keyless asynchronous covert communication," in *Proc. of IEEE Information Theory Workshop (ITW)*, Cambridge, UK, 2016, pp. 191–195.

VITA

Keerthi Suria Kumar Arumugam received his bachelors degree in Electronics and Communication Engineering from the College of Engineering - Guindy, Anna University, India, in 2013. He then joined the Masters program at the Georgia Institute of Technology and, in 2014, started working with Dr. Matthieu Bloch in the Communication Architectures Research group (ARCOM) to pursue his doctoral degree. His research interests include covert communication and wireless communication.